Original document

METHOD FOR ADJUSTING ACCESS TO PACKET EXCHANGE NETWORK

Publication number: JP10070574
Publication date: 1998-03-10
Inventor: BERTHAUD JEAN-MARC; FORIEL PIERRE-ANDRE; GALAND CLAUDE; STEPHEN LENGELLE; NICOLAS LAURENT
Applicant: IBM
Classification:
- international: *H04Q3/00; H04L12/24; H04L12/56;* **H04Q3/00; H04L12/24; H04L12/56;** (IPC1-7): H04L12/56; H04L12/28; H04Q3/00
- European:
Application number: JP19970162137 19970619
Priority number(s): EP19960480087 19960620

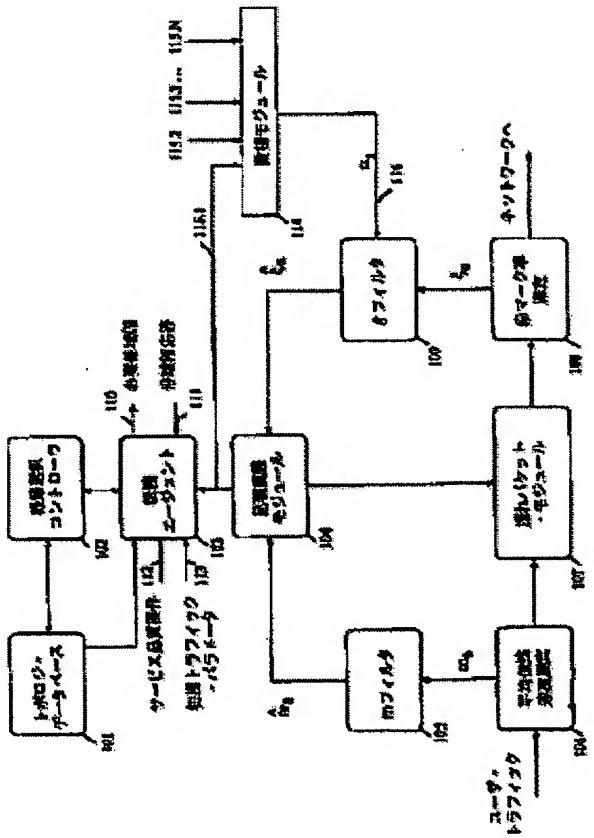
Also published as:
US5815492 (A1)

View INPADOC patent family
View list of citing documents

Report a data error here

Abstract of **JP10070574**

PROBLEM TO BE SOLVED: To ensure impartiality among all connections supported by a same processor by including processes which measure an average bit transfer speed, control traffic flows, measure a packet missing rate, filter it and request correction of a frequency band width thereby controlling the adjustment of a plurality of connections. SOLUTION: This method includes a process that measures the average bit transfer speed of a signal from a sender node, a process uses a leaked packet control circuit to control a traffic flow from the sender node to the network, a process that measures the missing rate of a packet brought into the network by the leaked packet control circuit, a process filters a missing rate measured value, a correction request process that corrects a frequency band width assigned for connection from the sender node, and a process that corrects a frequency band width of a missing rate measurement low pass filter based thereon.



Description of corresponding document: **US5815492**

Translate this text

TECHNICAL FIELD

The present invention relates to traffic management in high speed transmission networks, in particular to a method and system for monitoring traffic, for filtering traffic measurement and dynamically adjusting bandwidth allocated to connections.

BACKGROUND ART

Technology and Market Trends

The evolution of the telecommunications in general and of the packet switching networks in particular is driven by many factors among which two of them worth emphasizing: technologies and applications. Communication technologies have realized these last years considerable progress with:
the maturing of new transmission media and specially of optical fiber. High speed rates can now be sustained with very low bit error rates.
the universal use of digital technologies within private and public telecommunications networks.

The increase in communication capacity is generating more attractive tariffs and large bandwidths are economically more and more attractive. On the other hand, in relation with these new emerging technologies, many potential applications that were not possible before are now becoming accessible and attractive. In this environment, three generic requirements are expressed by the users:
improving old applications,
optimizing communication networks,
doing new applications.

High Speed Packet Switching Networks

Data transmission is now evolving with a specific focus on applications and by integrating a fundamental shift in the customer traffic profile. Driven by the growth of workstations, the local area networks interconnection, the distributed processing between workstations and super computers, the new applications and the integration of various and often conflicting structures--hierarchical versus peer to peer, wide versus local area networks, voice versus data--the data profile has become more bandwidth consuming, bursting, non-deterministic and requires more connectivity. Based on the above, there is strong requirement for supporting distributed computing applications across high speed networks that can carry local area network communications, voice, video, and traffic among channel attached hosts, business, engineering workstations, terminals, and small to intermediate file servers. This vision of a high speed multi-protocol network is the driver for the emergence of fast packet switching networks architectures in which data, voice, and video information is digitally encoded, chopped into small packets and transmitted through a common set of nodes and links.

An efficient transport of mixed traffic streams on very high speed lines means for these new network architectures a set of requirements in term of performance and resource consumption which can be summarized as follows:
very large flexibility to support a wide range of connectivity options,
very high throughput and a very short packet processing time,
efficient flow and congestion control.

Connectivity

In high speed networks, the nodes must provide a total connectivity. This includes attachment of the user's devices, regardless of vendor or protocol, and the ability to have the end user communicate with any other device. The network must support any type of traffic including data, voice, video, fax, graphic or image. Nodes must be able to take advantage of all common carrier facilities and to be adaptable to a plurality of protocols. All needed conversions must be automatic and transparent to the end user.

Throughput and Processing Time

One of the key requirement of high speed packet switching networks is to reduce the end-to-end delay in order to satisfy real time delivery constraints and to achieve the necessary high nodal throughput for the transport of voice and video. Increases in link speeds have not been matched by proportionate increases in the processing speeds of communication nodes and the fundamental challenge for high speed networks is to minimize the packet processing time within each node. In order to minimize the processing time and to take full advantage of the high speed/low error rate technologies, most of the transport and control functions provided by the new high bandwidth network architectures are performed on an end-to-end basis. The flow control and particularly the path selection and bandwidth management processes are managed by the access points of the network which reduces both the awareness and the function of the intermediate nodes.

Congestion and Flow Control

Communication networks have at their disposal limited resources to ensure an efficient packets transmission. An efficient

bandwidth management is essential to take full advantage of a high speed network. While transmission costs per byte continue to drop year after year, transmission costs are likely to continue to represent the major expense of operating future telecommunication networks as the demand for bandwidth increases. Thus considerable efforts have been spent on designing flow and congestion control processes, bandwidth reservation mechanisms, routing algorithms to manage the network bandwidth.

An ideal network should be able to transmit an useful traffic directly proportional to the traffic offered to the network and this as far as the maximum transmission capacity is reached. Beyond this limit, the network should operate at its maximum capacity whatever the demand is. In the reality, the operations diverge from the ideal for a certain number of reasons which are all related to the inefficient allocation of resources in overloaded environment. For the operating to be satisfactory, the network must be implemented so as to avoid congestion. The simplest solution obviously consists in over-sizing the equipment so as to be positioned in an operating zone which is distant from the congestion. This solution is generally not adopted for evident reasons of costs and it is necessary to apply a certain number of preventive measures among which the main ones are :
the flow control for regulating the emitting data rate of the calling subscriber at a rate compatible with what the receiver can absorb.
the load regulation for globally limiting the number of packets present in the network to avoid an overloading of the resources, and
the load balancing for fairly distributing the traffic over all the links of the network to avoid a local congestion in particular resources.

Congestion Control

Traffic Characteristics

In order to avoid congestion and insure adequate traffic flow in packet communication networks, it is common to control the access of packet sources to the network on an ongoing basis. In order to successfully control traffic access, it is necessary, first, to accurately characterize the traffic so as to provide appropriate bandwidth for carrying that traffic. Simple measurements which provide accurate estimates of the bandwidth requirements of a source are taught in U.S. Pat. No. 5,274,625 entitled "A Method for Capturing Traffic Behavior with Simple Measurements" (Derby et al.). In this application, the parameters used to characterize traffic are:
R, the peak bit rate of the incoming traffic in bits per second,
m, the mean bit rate of the incoming traffic in bits per second, and
b, the mean burst duration of the traffic in seconds.

Rather than using the actual burst duration, however, a so-called "exponential substitution" technique is used to calculate equivalent burst duration which would produce the same packet loss probability if the traffic were a well-behaved, exponentially distributed, on/off process. For traffic widely differing from such an exponential process, this equivalent burst duration produces a much more accurate characterization of the actual traffic and therefore permits a higher density of traffic on the same transmission facilities.

Leaky Bucket

The measured parameters are used to control the access of signal sources to the network when the actual traffic behavior departs significantly from the initial assumptions. A leaky bucket mechanism is one technique for controlling access to the network when the traffic exceeds the initial assumptions, but yet permits transparent access to the network when the traffic remains within these initial assumptions. One such leaky bucket mechanism is shown in U.S. Pat. No. 5,311,513 entitled "Rate-based Congestion Control in Packet Communications Networks" (Ahmadi et al.). More particularly, the leaky bucket mechanism prevents saturation of the network by low priority packets by limiting the number of low priority packets which can be transmitted in a fixed period of time while imposing a minimum on the number of red packets transmitted at a given time. Such leaky bucket control mechanisms optimize the low priority throughput of the packet network. High priority traffic, of course, is transmitted with little or no delay in the leaky bucket mechanism.

Traffic Monitoring

The above-described mechanisms are suitable for controlling traffic only if said traffic is reasonably well-behaved and remains within the general vicinity of the initially assumed traffic parameters. The traffic management system, however, must be structured to deal with traffic which is not well-behaved and which departs substantially from the initially assumed traffic parameters. If such a departure persists for any significant length of time, a new connection bandwidth must be assigned to the connection to accommodate the new traffic parameters. Such adaptation of the control system to radical changes in traffic behavior presents the problems of filtering the traffic measurements to separate transient changes of traffic behavior from longer term changes, and determining reasonable ranges within which the initially assumed traffic parameters can be maintained and outside of which new connection bandwidths must be requested. A bandwidth too large for the actual traffic is wasteful of connection resources while a bandwidth too small results in excessive packet loss. Ancillary problems include reasonable ease in implementation of the adaptation process and reasonable computational requirements in realizing the implementation.

Bandwidth Measurement and Adaptation

U.S. Pat. No. 5,359,593 entitled "Dynamic Bandwidth Estimation and Adaptation for Packet Communication Networks" (Derby et

al.) discloses a dynamic adaptation of a traffic control system to changes in the traffic parameters by defining a region within which adaptation is not required and outside of which a new bandwidth allocation must be requested. In particular, the bandwidth requirement is adjusted:
upward if the measurements indicate that either a desired maximum packet loss probability will be exceeded or if the traffic on that connection will start to unfairly interfere with other connections sharing the transmission facilities.
downward if significant bandwidth savings can be realized for both the user of the connection and for the balance of the network, without violating any quality of service guarantees for all of the connections.

These limits on the adaptation region are converted to values of effective mean burst duration b and mean bit rates m. The measured effective mean burst duration and mean bit rates are then filtered to insure that the filtered values are statistically reliable, i.e., that a sufficient number of raw measurements are involved to insure a preselected confidence level in the results. This minimum number of raw measurements, in turn, determines the amount of time required to collect the raw measurements, given the mean bit rate of the traffic. This measurement time can be used to measure not only the statistics of the incoming data stream to the leaky bucket, but also the effect of the leaky bucket on the incoming traffic. This latter measurement allows a measure of how well the leaky bucket is dealing with variances in the offered traffic and hence the packet loss probability. When the traffic parameters fall outside of the desired adaptation region, a new connection with a different bandwidth is requested in order to accommodate the changes in the traffic parameters.

The adaptation mechanism disclosed in U.S. Pat. No. 5,359,593 entitled "Dynamic Bandwidth Estimation and Adaptation for Packet Communication Networks" (Derby et al.) insures a continuously reasonable traffic management strategy when the offered traffic variations are small and slow. However, this mechanism presents some limitations when the traffic variations become more important and faster. Then, the adaptation mechanism requires a longer time to converge resulting in an over or under reservation of the bandwidth on the network.

A second limitation of the adaptation mechanism appears when more than one connection is monitored by a single processor which is usually the case in practice. Some connections may require more bandwidth adaptation than other connections within a given time period. The limited processing power of the processor may result in a lack of fairness which might be detrimental to the other connections.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to improve the mechanism disclosed in U.S. Pat. No. 5,359,593 in order to dynamically estimate and adapt the bandwidth for large and fast traffic variations.

It is a further object to control the adaptation of multiple connections and to ensure fairness between all connection supported by a same processor.

The present invention relates to a method and system of dynamically adapting access to a packet switching communication network comprising a plurality of nodes interconnected with transmission links for the transmission of digital traffic from source nodes to destination nodes, each node comprising one or a plurality of link processors for processing one or a plurality of links, said method comprising the steps of:
measuring the mean bit rate of traffic from said source node,
controlling the flow of said traffic from said source node into the network by means of a leaky bucket control circuit,
measuring the loss probability of packets introduced into said network by said leaky bucket control circuit,
filtering said loss probability measurements,
defining adaptation regions on the values of said simultaneous mean bit rate and loss probability measurements,
in response to pairs of said mean bit rate and loss probability measurements falling outside said adaptation regions, requesting a modification of the bandwidth allocated to connections from said source node,

said step of requesting a modification of the bandwidth comprising the further steps of:
measuring an average number of bandwidth modification requests for each link processor within the source node,
adapting, for all connections processed by the same processor within the source node, the bandwidth of the loss probability measurements' low pass filter according to the average number of bandwidth modification requests.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a general representation of the dynamic traffic management mechanism according to the present invention.

FIG. 2 shows a typical model of high speed packet switching network including the nodes claimed in the present invention.

FIG. 3 describes a high speed node according to the present invention.

FIG. 4 shows a graphical representation, in the mean bit rate/effective burst duration plane, of the adaptation region outside of which new connection parameters are requested for an existing connection in accordance with the present invention.

FIG. 5 shows a flow chart of the process for dynamically adapting bandwidth using the adaptation region illustrated in FIG. 4.

FIG. 6 shows a graphic representation of the flow control implemented by the Supervision module according to the present invention.

FIG. 7 shows a connection request message which might be used to set-up initial connections and dynamically altered connections using the dynamic traffic management mechanism of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

High Speed Communications

As illustrated in FIG. 2, a typical model of communication system is made of several user networks (212) communicating through a high performance network (200) using private lines, carrier provided services, or public data networks. Each user network can be described as a set of communication processors and links (211) interconnecting large computers used as enterprise servers (213), user groups using workstations or personal computers attached on LAN (Local Area Networks 214), applications servers (215), PBX (Private Branch exchange 216) or video servers (217). These user networks, dispersed in different establishments, need to be interconnected through wide area transport facilities and different approaches can be used for organizing the data transfer. Some architectures involve the checking for data integrity at each network node, thus slowing down the transmission. Others are essentially looking for a high speed data transfer and to that end the transmission, routing and switching techniques within the nodes are optimized to process the flowing packets towards their final destination at the highest possible rate. The present invention belongs essentially to the latter category and more particularly to the fast packet switching network architecture detailed in the following paragraphs.

High Performance Packet Switching Networks

The general view in FIG. 2 shows a fast packet switching transmission system comprising eight nodes (201 to 208) each node being interconnected by means of high speed communication lines called Trunks (209). The access (210) to the high speed network by the users is realized through Access Nodes (202 to 205) located at the periphery. These Access Nodes comprise one or more Ports, each one providing an access point for attaching external devices supporting standard interfaces to the network and performing the conversions required to transport the users data flow across the network from and to other external devices. As example, the Access Node 202 interfaces respectively a Private Branch exchange (PBX), an application server and a hub through three Ports and communicates through the network by means of the adjacent Transit Nodes 201, 206 and 208.

Switching Nodes

Each network node (201 to 208) includes a Routing Point where the incoming data packets are selectively routed on the outgoing Trunks towards the neighboring Transit Nodes. Such routing decisions are made according to the information contained in the header of the data packets. In addition to the basic packet routing function, the network nodes also provide ancillary services such as:
the determination of routing paths for packets originated in the node,
directory services like retrieving and updating information about network users and resources,
the maintaining of a consistent view of the physical network topology, including link utilization information, and
the reservation of resources at access points of the network.

Each Port is connected to a plurality of user processing equipment, each user equipment comprising either a source of digital data to be transmitted to another user system, or a data sink for consuming digital data received from another user system, or, typically, both. The interpretation of the users protocols, the translation of the users data into packets formatted appropriately for their transmission on the packet network (200) and the generation of a header to route these packets are executed by an Access Agent running in the Port. This header is made of Control and Routing Fields.
The Routing Fields contain all the information necessary to route the packet through the network (200) to the destination node to which it is addressed. These fields can take several formats depending on the routing mode specified (connection oriented or connectionless routing mode).
The Control Fields include, among other things, an encoded identification of the protocol to be used in interpreting the Routing Fields.

Routing Points

FIG. 3 shows a general block diagram of a typical Routing Point (300) such as it can be found in the network nodes (201 to 208) illustrated in FIG. 2. A Routing Point comprises a high speed packet Switch (302) onto which packets arriving at the Routing Point are entered. Such packets are received:
from other nodes over high speed transmission links (303) via Trunk Adapters (304).
from users via application adapters called Ports (301).

Using information in the packet header, the adapters (304, 301) determine which packets are to be routed by means of the Switch (302) towards a local user network (307) or towards a transmission link (303) leaving the node. The adapters (301 and 304) include queuing circuits for queuing packets prior to or subsequent to their launch on the Switch (302).

The Route Controller (305) calculates the optimum paths through the network (200) so as to satisfy a given set of quality of service specified by the user and to minimize the amount of network resources used to complete the communication path. Then, it builds the header of the packets generated in the Routing Point. The optimization criterion includes the number of intermediate nodes, the characteristics of the connection request, the capabilities and the utilization of the Trunks in the path, the quality of service specified for this connection . . .

All the information necessary for the routing, about the nodes and transmission links connected to the nodes, are contained in a Network Topology Database (306). Under steady state conditions, every Routing Point has the same view of the network. The network topology information is updated when new links are activated, new nodes added to the network, when links or nodes are dropped or when link loads change significantly. Such information is originated at the network node to which the resources are attached and is exchanged by means of control messages with all other Path Servers to provide the up-to-date topological information needed for path selection (such database updates are carried on packets very similar to the data packets exchanged between end users of the network). The fact that the network topology is kept current in every node through continuous updates allows dynamic network reconfigurations without disrupting end users logical connections (sessions).

The incoming transmission links to the packet Routing Point may comprise links from external devices in the local user networks (210) or links (Trunks) from adjacent network nodes (209). In any case, the Routing Point operates in the same manner to receive each data packet and forward it on to another Routing Point as dictated by the information in the packet header. The fast packet switching network operates to enable a communication between any two end user applications without dedicating any transmission or node facilities to that communication path except for the duration of a single packet. In this way, the utilization of the communication facilities of the packet network is optimized to carry significantly more traffic than would be possible with dedicated transmission links for each communication path.

Network Control Functions

The Network Control Functions are those that control, allocate, and manage the resources of the physical network. Each Routing Point has a set of the foregoing functions in the Route Controller (305) and uses it to facilitate the establishment and the maintenance of the connections between users applications. The Network Control Functions include in particular:
Directory Services for retrieving and maintaining information about network users and resources.
Bandwidth Management for processing the bandwidth reservation and maintenance messages, and for monitoring the current reservation levels on links.
Path Selection for choosing the best path for each new connection considering the connection requirements and the current link utilization levels.
a Control Spanning Tree for establishing and maintaining a routing tree among the network nodes, to distribute control information (in parallel) including link utilization, and for updating the Topology Database of the nodes with new network configurations or link/node failures.
a Topology Update for distributing and maintaining, in every node, information about the logical and physical network (including link utilization information) using the Spanning Tree.
Congestion Control for enforcing the bandwidth reservation agreements between the network's users and the network which are established at the call set-up time, and for estimating actual bandwidth and for adjusting reservation if necessary during the life of the connection.

Congestion Control

The Network Control Functions provide a quality of service guarantee and when required, a bandwidth guarantee to every transport connection established across the network. When a transport connection with specified bandwidth is set-up, an interaction between the network and the connection initiator results in either a guaranteed bandwidth being reserved for this connection or the connection being blocked due to lack of network resources. Once the set-up is complete and the transmission starts, the congestion control mechanism ensures that the traffic going into the network stays within the allocated bandwidth by controlling its burstiness and ensuring some long term average bit rate for the link. When a connection specifies a required bandwidth at connection set-up time, it requires its own congestion control mechanism, and it is assigned to a network connection of its own. The basic preventive congestion control strategy consists of a leaky bucket operating at the access node of each connection with the objective of guarantying users that their reserved level of traffic will cross the network with bounded delay and with an extremely small probability of packet loss due to congestion in intermediate nodes (in the order of 10@-6). The simplest way to provide for low/no packet loss would be to reserve the entire bandwidth of the user connection. For bursty user traffic, however, this approach can waste a significant amount of bandwidth across the network. Thus, an approach is to reserve a bandwidth amount equal to the "equivalent capacity" needed by the user. The basic idea is that the reservation mechanism derives a level of reservation from the knowledge of the source characteristics and of the network status. This reservation level falls somewhere between the average bandwidth required by the user and the maximum capacity of the connection. For more bursty connections this reservation level needs to be higher than it is for less bursty connections to guarantee the same discard probability.

Because most traffic flows on bandwidth reserved connections, it is essential to estimate the required bandwidth for users who can't do it themselves. For example it would be extremely difficult for customers to define the required bandwidth for traffic entering the network from a LAN server. Thus, considerable work has been done to estimate the user traffic and the utilization of the links and to determine what measurements to take and what filters to use to determine when and how to change the leaky

bucket parameters for a detected change in user bandwidth requirements. The congestion control mechanism monitors user traffic streams and makes changes to the reserved bandwidth when necessary either to guarantee the loss probability as user demand increases or to use bandwidth more efficiently as user demand decrease. It is recognized that a particular challenge in this regard is to avoid adjusting bandwidth reservation too often, because significant changes could require new path selection and bandwidth management flows across the network and frequent changes could lead to a network thrashing condition.

Connection Request

In order to transmit packets on the network, it is necessary to calculate a feasible path or route through the network from the source node to the destination node for the transmission of such packets. To avoid overload on any of the links on this route, the route is calculated in accordance with an algorithm that insures that adequate bandwidth is available for the new connection. One such algorithm is disclosed in U.S. Pat. No. 5,233,604 entitled "Method and Apparatus for Optimum Path Selection in Packet Transmission Networks" (Ahmadi et al.). Once such a route is calculated, a connection request message is launched on the network, following the computed route and updating the bandwidth occupancy of each link along the route to reflect the new connection.

FIG. 7 shows a graphical representation of a connection request message to be launched from a source node to a destination node along a pre-calculated route. The connection message comprises a routing field (700) which includes the information necessary to transmit the connection message along the pre-calculated route. Also included in the connection request message is a connection request vector (701) which characterizes the important statistical characteristics of the new packet source and which allows this new source to be statistically multiplexed with the previously existing signals on each link of the route. As will be discussed in detail hereinafter, the connection request vector includes a relatively few parameters necessary to adequately characterize the packet source. As described in U.S. Pat. No. 5,311,513 entitled "Rate-based Congestion in Packet Communications Networks" (Ahmadi et al.), these parameters might include:
R the maximum bit rate for the source,
m, the mean of that bit rate, and
b, the equivalent burst duration of packets from that source.

The values in the connection request vector are used to test each link of the route to determine if the new connection can actually be supported by that link, and to update, separately for each link, the link occupancy metric for that link to reflect the addition of the new connection. If the link occupancy has changed since the route was calculated, the connection may be rejected at any node along the route, and the source node notified of the rejection. Finally, the control fields (702) include additional information used in establishing the connection, but which is not pertinent to the present invention and will not be further discussed here. Note that, when a connection is to be taken down, a connection removal message having the same format as FIG. 7 is transmitted along the route of the connection to be removed. The link occupancy of each link is then updated to reflect the removal of this connection by subtracting the metrics for the removed connection.

Source Bandwidth Management

The Source Bandwidth Management system shown in FIG. 1 is provided for each source of user traffic to be applied to the network (200). These bandwidth management systems are located in the access nodes and one such a system is provided for each direction of transmission between two communicating users. Although such systems can be realized with hard-wired circuit components, the preferred embodiment utilizes a programmed computer since such an implementation is more readily modified to accommodate improvements and to reflect changes in traffic patterns.

Before proceeding further to a detailed description of the Source Bandwidth Management shown FIG. 1, the following variables will be defined:
R: The maximum bit rate, in bits per second, of the input traffic as requested by the user source to initiate the connection.
m: The mean bit rate, in bits per second, of the input traffic as requested by the user source to initiate or to adapt the connection.
b: The mean burst duration, in seconds, of the input traffic as requested by the user source to initiate or to adapt the connection.
t: The sampling period of both m and .xi. Filters (105 and 109). Filters receive measurements and report filtered

outputs mn and @.xi..sbsp.n to the Estimation and Adaptation module (104) every t seconds.
mn : The raw measurement of the mean bit rate of the input traffic for the nth sampling period of duration t.
.xi.n : The raw measurement of the red marking probability being observed in the Leaky Bucket module (107) during the nth sampling period of duration t.
@m.sbsp.n : The filtered value of the mean bit rate m, as filtered by bit rate m Filter (105) of FIG. 1, for the input traffic at the end of the nth sampling period.
@.xi..sbsp.n : The filtered value of the red marking probability, as filtered by red marking probability .xi. Filter (109) of FIG. 1 for the leaky bucket at the end of the nth sampling period.
.gamma.: The green token generation rate currently used in the Leaky Bucket module (107) of FIG. 1. The green token rate determines the rate at which packets marked green can be injected into the network. It is assumed that a bandwidth amount of .gamma. (equivalent capacity) has been reserved in the network for this connection.
M: The maximum size of the green token pool in the Leaky Bucket module (107) of FIG. 1. The size of the green token pool determines the length of green packets injected into the network.

Connection Agent Module

As described in FIG. 1, in connection with FIG. 2, when a new connection is to be set-up through network (200), an initial estimate of the traffic characteristics is made by the packet source. This estimate arrives at the bandwidth management system of FIG. 1 on link (113) together with the quality-of-service (QOS) requirements on link (112). Such quality-of-service requirements include among other things: acceptable loss probabilities, acceptable delays, and real-time delivery requirements.

A Connection Agent (103) passes these connection requirements on to Path Selection Controller (102). The latter uses these requirements, together with the up-to-date network description stored in the Topology Database (101), to calculate a bandwidth (equivalent capacity) .gamma. and a connection path through network (200) satisfying all of these requirements. One optimum Path Selection Controller is described in U.S. Pat. No. 5,233,604 entitled "Method and Apparatus for Optimum Path Selection in Packet Transmission Networks" (Ahmadi et al.). Once calculated, the proposed connection path is encoded in a Connection Request Message such as the message shown in FIG. 7 and is launched as a bandwidth request on link (110) onto the network (200). The bandwidth request message of FIG. 7 traverses the calculated connection path and, at each node along the route, is used to reserve, in the next link of the connection, the bandwidth required to satisfy the connection request.

If sufficient bandwidth is available in each link of the connection along the computed path, the destination node receives the request and transmits back an acceptance of the new connection. If, at any link along the route, insufficient bandwidth is available due to changes in the traffic patterns, a denial of the connection request is transmitted back to the source end node.

These bandwidth replies, whether negative or positive, are delivered back to Connection Agent (103) on link (111). If the connection is denied, the user source is notified and another attempt at the connection can be made later. If the connection is accepted, Leaky Bucket Module (107) is activated and supplied with the appropriate parameters to control the access of the user traffic. The user then begins introducing traffic.

Leaky Bucket Module

The source bandwidth management system comprises a Leaky Bucket module (107) to which the user traffic on input link is applied. The output of Leaky Bucket module (107) is applied to the network (200) of FIG. 2. In the Leaky Bucket module (107), packets are launched into the network with one of at least two different priority classes, conventionally called "red" and "green", where green is the higher priority.

Green packets are guaranteed a pre-specified grade of service based on an acceptable level of delay and loss probability within the network. Red packets do not have the same guarantees and are discarded before the green packets when congestion occurs.

Strategies for optimally marking packets in a leaky bucket mechanism are disclosed in U.S. Pat. No. 5,311,513 entitled "Rate-based Congestion Control in Packet Communications Networks" (Ahmadi et al.). The function of the Leaky Bucket module (107) is to "shape" the traffic before it enters the network (200). User packets not conforming to the initially provided statistical description, are marked red or discarded. For a connection that is characterized by its peak rate R, its mean rate m, and its average burst duration b, four parameters are computed and used in the Leaky Bucket module (107) to control that the bandwidth demand of the connection does not exceed the amount of bandwidth that has been actually reserved in the network for this connection.
* .gamma. Green Token Generation Rate
Its value is determined by relation (1): ##EQU1## where X is the amount of buffer space (in bits) available on each Trunk adapter (304) along the path of the connection.
.epsilon. is the target maximum packet loss probability in the network,

y=ln(1/.epsilon.)b(1-.rho.)R, and

.rho.=m/R (.rho. denotes the utilization of the source).

For simplicity, it is assumed that all the buffer sizes are the same(X) and that the target maximum packet loss probabilities for each link are the same, .epsilon..
* M: Maximum Green Pool Size
Its value is determined by relation (2): ##EQU2## where .xi.T is the target red marking probability (in the preferred embodiment, .xi.T =0.01), and
Max-- packet represents the maximum size of a packet at the network access.
* .gamma.R : Red Token Generation Rate

Its value .gamma.R is set to a fraction of the green token generation rate. In the preferred embodiment, this fraction is set to 10% .gamma. is given by relation (3):

.gamma.R =0.1 .gamma.
* MR : Maximum Red Pool Size
Its value is determined by relation (4):

MR =M

At the establishment of the connection, a bandwidth amount .gamma. is reserved in the network by the Connection Agent module (103) and the leaky bucket parameters are initialized.

The green token pool is set to its maximum value M as given by relation (2), and is continuously refreshed at the rate .gamma. given by relation (1): the pool receives y bits per second.

Similarly, the red token pool is set to its maximum value MR as given by relation (4), and is continuously refreshed at the rate .gamma.r given by relation (3).

For each new incoming packet, the Leaky Bucket module (107) checks whether there is enough green token in its green pool. If yes, then the packet is tagged "green" and is immediately transmitted to the network. Else, the Leaky Bucket module (107) checks whether the red pool contains enough tokens. If yes, the packet is tagged as discardable ("red") and transmitted to the network. Else, it is discarded, or optionally spaced for a period that would allow the pool to contain enough green or red token to allow the packet to be transmitted.

If the traffic characteristics remain within the initially negotiated values, however, the red marking mechanism is sufficiently limited to insure the promised loss probability. If the incoming traffic characteristics depart substantially from the negotiated values, Estimation and Adaptation module (104) is invoked to take corrective actions, to either increase or decrease the bandwidth reservation as will be discussed later.

Estimation and Adaptation Module

When the connection is accepted, the Leaky Bucket module (107) is activated and the user then begins introducing traffic. At the same time, Estimation and Adaptation module (104) begins monitoring this incoming traffic to determine if any significant changes in the incoming traffic characteristics have occurred during the life of the connection. If so, Estimation and Adaptation module (104) notifies Connection Agent (103) to request a new bandwidth allocation, supplying Connection Agent (103) with the new traffic parameters required for the connection. As before, Connection Agent (103) launches a new bandwidth request on link (110) requesting a bandwidth adjustment for said connection. If the adjustment is accepted, the leaky bucket paramters are updated with the new traffic characteristics and Estimation and Adaptation module (104 continues to monitor the incoming traffic, but with the new characteristics.

Note that only a new bandwidth allocation is requested, rather than a new connection. This saves the overhead involved in taking down the old connection and setting up a new connection. If the requested additional bandwidth is not available, the connection can be either taken down or given a lower priority, depending on the original negotiations with the sending party at the source node.

Bandwidth Measurement and Filtering

Referring to FIG. 1, measuring the mean bit rate mm of the incoming traffic in Measurement module (106) is simple. A counter counts the number of bits received during the sampling period t and divides this number by the length t. Similarly, the red marking probability .xi.n is equal to the number of packets marked red during the sampling period t divided by the total number of packets transmitted during the period t. These raw data are delivered to the m filter (105) and the .xi. Filter (109), the latter being a low pass filter, every t seconds. The function of the m and .xi. Filters (105 and 109) is to filter out transient changes in mean bit rate mn and red marking probability .xi.. The filters (105) and (109) report estimates of mean bit rate and red marking probabilities, respectively, every t second. Each filter (105) or (109) maps the current raw measurement and all of the previous measurements into an estimate of the filtered value. Let x1, x2, . . . , xn be the raw measurements and x1, x2, . . . , xn be the estimates (where x is either m or .xi.). While the mapping of filters (105) and (109) can be any function, in the preferred embodiment of the present invention, this mapping is exponential. The nth estimate xn is given by:

xn =.alpha.x(n-1) +(1-.alpha.)xn

where the filter parameter .alpha., lying between zero and one (0<.alpha.<1), determines the relative reliability of the two terms in the above equation. The value of .alpha. is set to a constant equal to 0.8 for the m Filter (105). For the .xi. Filter (109), the value of .alpha. on whether the raw value .xi.n is greater than the filtered value .xi.n :
if .xi.n <.xi.n, then .alpha.=0.8 (nominal value),

else a=as, where .alpha.s is a parameter provided by the Supervision module (114) on link (116) as explained later.

Filtered values @m.sbsp.n and @.xi..sbsp.n of the mean bit rate and the red marking probability are delivered to the Estimation and Adaptation module (104) once every t seconds. These filtered values are compared in the Estimation and Adaptation module (104) to acceptable values to determine whether or not an adaptation is required, that is a new connection request is warranted. This comparison will be discussed in connection with the adaptation region disclosed graphically in FIG. 4.

Adaptation Regions

FIG. 4 shows the regions used to adapt the bandwidth of a connection in response to changes in the mean bit rate m and/or the red marking probability .xi. as they are estimated at the network port by means of modules (106), (105), (108), and (109) detailed above. FIG. 4 includes three regions in a two dimension plane:

Adjust-up region (602) defined by:

.xi.n >.xi.H

where .xi.H is a constant, which is equal to 5.10@-2 in the preferred embodiment. Region (602) is further divided into two sub-areas:
* for mn .ltoreq..gamma. (602a)
* for mn .ltoreq..gamma. (602b)

Adjust-down region (601), defined by:

.xi.n <.xi.L

mn <.gamma.

where .xi.L is a constant equal to 10@-2 in the preferred embodiment. Region (601) is further divided into two sub-areas:
* for mn .ltoreq..beta..m(601a)
* for mn >.beta..m(601b)

where .beta. is a constant equal to 0.3 in the preferred embodiment.

Dynamic Bandwidth Adaptation

Every t seconds, the Estimation and Adaptation module (104) checks the position of the filtered values mn and .xi.n and in accordance with the adaptation regions, decides to either adjust up or down, or not adapt the connection bandwidth. This decision is taken according to the algorithm shown in FIG. 5.

*(501) A test determines where the point of coordinates (mn,.xi.n) lies on the plane.

(512) If the point lies in the "no-adjust" region (604), then no adaptation is attempted and the algorithm is completed.

(505) If the point lies in the "adjust up" region (602), then a second test (505) positions the point (mn, .xi.n) in one of the sub-areas:

(507) If the point lies in sub area (602a), then a new value of the burst parameter b is estimated by means of the exponential substitution method disclosed in U.S. Pat. No. 5,359,593 entitled "Dynamic Bandwidth Estimation and Adaptation for Packet Communications Networks" (Derby et al.) b is given by relation (5): ##EQU3##

*(506) If the point lies in sub-area (602b), then a new value of the burst parameter b is computed:

b=b-- max

where b-- max is the maximum burst size that is supported by this implementation. In the preferred implementation b-- max=10 ms.

(502) If the point lies in the "adjust-down" region 601), then a counter n-- Low is incremented and tested (503).

(512) If the updated value of the counter is less than a constant N-- Low taken to 5 in the preferred embodiment, then the algorithm is completed. The incrementation of the counter (502) and the test (503) avoid making too fast adjust-down decisions during transient states.

(504) If the point lies in the "adjust-down" region (601) for N-- Low periods t, then a test (504) determines the position of the point in one of the two sub-areas (601a) or (601b).

(508) If the point lies in sub-area (601a), then a new value of the burst parameter b is computed:

b=b/c

where c is a constant >1 (c=2 in the preferred embodiment).

(507) If the point lies in sub-area (601b), then a new value of the burst parameter b is computed by means of equation (5).

(509) Once a new value of the burst parameter b has been determined either in steps (506), (507) or (508),a new value of the green

token generation rate .gamma. is computed:

m=mn ##EQU4##

(510) Then, the regions of FIG. 4 are updated:

the upper boundary (603) of the "adjust-down" region (601) and the medium boundary (605) of the "adjust-up" region (602) are set to the new value of .gamma., and

the medium boundary (604) of the "adjust-down" region (601) is set to .beta..m.

(511) The bandwidth request message of FIG. 7 is sent out on link (110) to the network and is delivered to every node on the path for adjusting the bandwidth reserved to the connection.

Adaptation Control and Fairness for Multiple Connections

The above described algorithm is an improvement for large and fast traffic variations of the method and system disclosed in U.S. Pat. No. 5,359,593 entitled "Dynamic Bandwidth Estimation and Adaptation for Packet Communication Networks" (Derby et al.). In particular, the present invention supports two important features: a global control of the number of connections that can be adapted by the processor, given its processing capability, and a fairness between connections. These features are supported thanks to a Supervision module (114), implemented on top of the dynamic traffic management mechanism as shown in FIG. 1.

Adaptation Control

The global control of the number of connections is implemented as follows. At each sampling period t, the Supervision module (114) receives n bandwidth requests on links (115.1), (115.2), . . . , (115.N), with:

0.ltoreq.n.ltoreq.N

where N is the total number of connections served by the processor.

The average number n of bandwidth requests in the last periods is estimated by a filtering operation to:

n=0.99.+-.n0.01n

Then the filtered value n is checked against predefined thresholds. Let No be the processing capability of the processor (number of adaptations per seconds), the following tests are performed:
if n<0.25No, then .varies.s =0.4: the filter coefficient .varies.s is relaxed to a very loose value that enables fast variations of the average red marking probability as estimated by the .xi. (low pass) Filter (109).
if 0.25No .ltoreq.n.ltoreq.0.5No then .varies.s 0.6:.varies.s is set to a loose value that makes variations of the red marking probability .xi.n slower.
if 0.5No .ltoreq.n.ltoreq.0.75No, then .varies.s =0.8:.varies.s is set to its nominal value.
if 0.75No .ltoreq.n, then .varies.s =0.95:.varies.s is set to a tight value which virtually freezes the average red marking probability .xi.n, so that displacements in the plane of FIG. 4 become very slow.

The coefficient .varies.s is then forwarded to the red marking probability .xi. Filter (109) via the line (116) for tuning its characteristics. This operation increases the fairness among connections. Indeed if a connection is much more demanding than the others in term of number of bandwidth adjustments per time unit, the coefficient s computed by the Supervision module (114), will increase, and therefore the trajectory of the connections in the adjust down region (601) of FIG. 4 will take more time, which will in turn force the average number of bandwidth adaptations per second to converge to No. FIG. 6 graphically illustrates the principle of the Supervision module and shows the time variations of the average number n of bandwidth requests. Four regions are defined for controlling the filter parameter .alpha.s according to the above algorithm:
* region (801), for very tight filter coefficient .alpha.s,
* region (802), for tight filter coefficient .alpha.s,
* region (803), for nominal filter coefficient .alpha.s,
* region (804), for loose filter coefficient .alpha.s.

Adaptation Fairness

The fairness between connections is implemented as follows. For each connection i supported by the adapter (0.ltoreq.i.ltoreq.N), the processor maintains a fairness variable Fi, which reflects the current behavior of this connection. This fairness variable is initialized at the connection set-up by:

Fi =1/No,

At each sampling period t, the processor performs the following operations for every connection (i=1, . . . , N):

First, the fairness variable Fi is updated
Fi =0.99Fi if connection i does not require a new bandwidth request, or
Fi =0.99Fi +0.01 if connection requires a new bandwidth request.

Second, the fairness variable Fi is tested. If
Fi >.delta./No, where .delta. is a constant equal to 1 in the preferred embodiment, then the connection i is no longer considered as a fair connection and as such should not be adapted, whatever its bandwidth demand, until the counter Fi decreases below the limit .delta./No.

This mechanism ensures fairness between connections in the sense that it prevents a single connection to use on the average a portion of the processor computational capacity greater than 1/No, that can be called the processor per connection fair share. A value of .delta. greater than 1 can be used to overbook the processor resource.

Claims of corresponding document: **US5815492**

We claim:

1. A method for dynamically controlling access by data sources to a packet data communication network interconnecting source and destination nodes, each source node having at least one management system for controlling access to the network by a data source connected to the source node, including for each said data source the steps of:
measuring the mean bit rate of the traffic emanating from the data source;
controlling the flow of data packets from the data source into the network;
measuring the loss probability of data packets introduced into the network;
performing a low pass filter operation on the loss probability measurements;
defining adaption regions based on the simultaneous mean bit rate and loss probability measurements;
in response to pairs of said mean bit rate and loss probability measurements falling outside the adaption regions, requesting modification of the bandwidth allocated to the transmission of data packets;
measuring the average number of bandwidth modification requests; and
modifying the characteristics of the low pass filtering step as a function of the average number of bandwidth modification requests.

2. The method according to claim 1 wherein said step of measuring an average number of bandwidth modification requests comprises the further step of:
filtering said average number of bandwidth modification request measurements.

3. The method according to claim 1 wherein: the more the average number of bandwidth modifications requested for the same processor increases, the more the bandwidth of the low pass filter (109) decreases.

4. The method according to claim 1 wherein
the more often a connection requires modification of its allocated bandwidth, the less the management system gives priority to said requests, and
the less often a connection requires modification of its allocated bandwidth, the more the link processor gives priority to said requests.

5. In a packet data communication network for interconnecting source and destination nodes, at least one management system, each for controlling access to the network by a data source connected to the source node comprising:
means for measuring the mean bit rate of the traffic emanating from the data source;
a leaky bucket circuit for controlling the flow of data packets from the data source into the network;
means for measuring the loss probability of data packets introduced into the network;
a low pass filter for filtering the loss probability measurements;
means for defining adaption regions based on the simultaneous mean bit rate and loss probability measurements;
means responsive to pairs of said mean bit rate and loss probability measurements falling outside the adaption regions for requesting modification of the bandwidth allocated to the transmission of data packets;
means for measuring the average number of bandwidth modification requests; and
means for modifying the characteristics of the low pass filter as a function of the average number of bandwidth modification requests.

6. A communications network according to claim 5 further comprising means for filtering said average number of bandwidth modification request measurements.

---

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－70574

(43)公開日　平成10年(1998)３月10日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　12/56		9744－5K	Ｈ０４Ｌ	11/20	１０２Ｃ
12/28			Ｈ０４Ｑ	3/00	
Ｈ０４Ｑ　3/00		9744－5K	Ｈ０４Ｌ	11/20	Ｇ

審査請求　未請求　請求項の数６　ＯＬ　（全 17 頁）

(21)出願番号　特願平9－162137

(22)出願日　平成９年(1997)６月19日

(31)優先権主張番号　９６４８００８７．４

(32)優先日　1996年６月20日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　ジャン＝マルク・ベルトー
フランス06270　ヴィユヌーブ・ルーベ　レ・アモー・デュ・ソレイユ　ル・ポッティチェリ

(74)代理人　弁理士　坂口　博　（外１名）

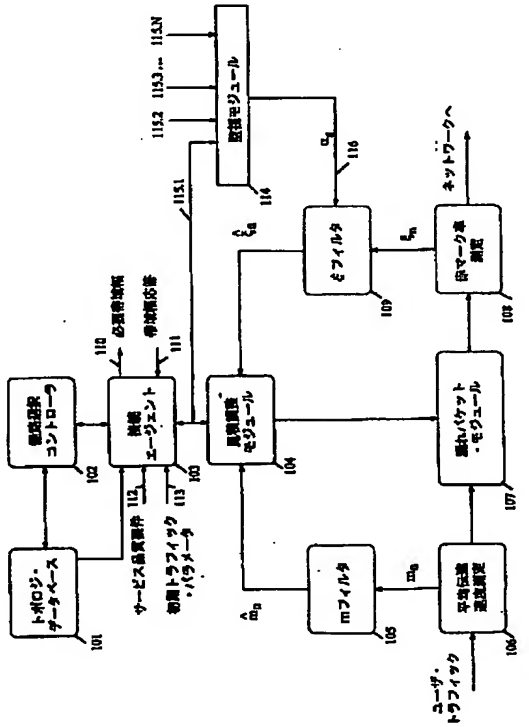
最終頁に続く

(54)【発明の名称】　パケット交換網へのアクセス調整方法

(57)【要約】

【課題】　信号源の平均ビット伝送速度と接続の紛失率を絶えず監視する動的帯域幅調整機構を含むパケット交換網へのアクセスを調整する方法およびシステム。

【解決手段】　上記の値をフィルタリングして雑音を除去してから使用して、値が平均ビット伝送速度、紛失率の面内の所定の許容可能調整領域に入るかどうかをテストする。この領域に入らない値があれば、帯域幅調整手続きが起動され、その結果、新しい接続帯域幅が獲得され、調整機構の新しいパラメータが決定される。さらに、この機構は、プロセッサの処理能力があると仮定して、１つのプロセッサによって調整可能な接続の数を制御する。この機構は、単一の接続が平均してプロセッサ能力のかなりの部分を使用するのを防ぐ。



1

【特許請求の範囲】

【請求項１】各ノードが１つまたは複数のリンクを処理する１つまたは複数のリンク・プロセッサを含む、送信元ノードから宛先ノードへのデジタル・トラフィックの伝送のために伝送リンク（２０９）によって相互接続された複数（２０１．．２０８）のノードを含むパケット交換通信網（２００）へのアクセスを動的に調整する方法であって、

前記送信元ノードからのトラフィックの平均ビット伝送速度を測定するステップ（１０６）と、

漏れバケット制御回路を使用して前記送信元ノードからネットワークへの前記トラフィックのフローを制御するステップ（１０７）と、

前記漏れバケット制御回路によって前記ネットワークにもたらされるパケットの紛失率を測定するステップ（１０８）と、

前記紛失率測定値をフィルタリングするステップ（１０９）と、

前記同時平均ビット伝送速度および紛失率測定の値に対して調整領域を定義するステップと、

前記調整領域内に収まらない前記平均ビット伝送速度および損失率測定の対に応答して、前記送信元ノードからの接続に割り振られた帯域幅の修正を要求するステップとを含み、

帯域幅の修正を要求する前記ステップが、

送信元ノード内の各リンク・プロセッサについて帯域幅修正要求の平均数を測定するステップと、

送信元ノード内の同一プロセッサによって処理されるすべての接続のために、帯域幅修正要求の前記平均数に従って紛失率測定低域フィルタの帯域幅を調整するステップとを含む方法。

【請求項２】帯域幅修正要求の平均数を測定する前記ステップが、

帯域幅修正要求測定値の前記平均数をフィルタリングするステップをさらに含むことを特徴とする、請求項１に記載の方法。

【請求項３】同じプロセッサへの帯域幅修正要求平均数が多くなるほど、低域フィルタ（１０９）の帯域幅が減少することを特徴とする、請求項１または２に記載の方法。

【請求項４】接続がそれに割り振られた帯域幅の修正を必要とする頻度が高いほど、リンク・プロセッサが前記要求に与える優先度が低くなり、

接続がそれに割り振られた帯域幅の修正を必要とする頻度が低いほど、リンク・プロセッサが前記要求に与える優先度が高くなることを特徴とする、請求項１ないし３のいずれか一項に記載の方法。

【請求項５】請求項１ないし４のいずれか一項に記載の伝送リンク（２０９）で相互接続された複数のノード（２０１．．２０８）を含むパケット交換通信網（２００）へのアクセスを調整する方法を実行する手段を含む通信ノード（３００）。

2

【請求項６】請求項５に記載の複数のノード（２０１．．２０８）を相互接続する複数の伝送リンクを含むパケット交換通信網（２００）。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、高速伝送網におけるトラフィック管理に関し、詳細にはトラフィックを監視し、トラフィック測定値をフィルタリングし、接続に割り振られる帯域幅を動的に調整する方法およびシステムに係わる。

【０００２】一般には遠隔通信、特にパケット交換網の発展は、多くの要因によって促進されるが、その中でも技法とアプリケーションの２つの要因は強調するに値する。

【０００３】通信技法は以下の要因によって最近数年間に著しい発展を実現している。

・新しい伝送媒体、特に光ファイバの成熟。きわめて低いビット誤り率で高速速度を維持することができるようになっている。

・構内通信網と公衆通信網内でのデジタル技法の一般的使用。

【０００４】通信容量の増大によって、さらに魅力的なトラフィックと広い帯域幅が経済的にますます魅力的になりつつある。一方、これらの新たに登場した技法に関係して、これまで不可能だった多くの潜在的アプリケーションが現在では利用可能になり、魅力的になっている。

・古いアプリケーションの改良

・通信網の最適化

・新しい応用の実施

【０００５】

【従来の技術】データ伝送は、現在、アプリケーションに特に重点を置き、顧客トラフィック・プロファイルに基本的シフトを組み込むことによって発展しつつある。ワークステーションの発達、ローカル・エリア・ネットワーク相互接続、ワークステーションおよびスーパー・コンピュータ間の分散処理、新しいアプリケーションと多様でしばしば競合し合う構造（階層構造対対等構造ピア、広域ネットワーク対ローカル・エリア・ネットワーク、音声対データ）の統合に促されて、データ・プロファイルはますます帯域幅を消費し、バースト化し、不確定的になっており、より多くの接続性を必要とするようになっている。上記に基づき、ホスト、ビジネス用、エンジニアリング・ワークステーション、端末、および小型から中型までのファイルサーバの間で、ローカル・エリア・ネットワーク通信、音声、ビデオ、およびトラフィックを伝送することができる高速網を介した分散コンピューティング・アプリケーションをサポートする必要

が増大している。このような高速マルチプロトコル網の展望は、データ、音声、およびビデオ情報をデジタル・コード化し、小型パケットに分割してノードおよびリンクの共通のセットを介して伝送する、高速パケット網アーキテクチャの登場の推進要因である。

【０００６】混在トラフィック・ストリームを超高速回線で効率的に伝送することは、これらの新しいネットワーク・アーキテクチャにとって、パフォーマンスと資源消費に関する一連の必要条件を意味し、これは以下のように要約される。

・広範囲な接続性オプションに対応するきわめて高い柔軟性

・きわめて高いスループットときわめて短いパケット処理時間

・フローおよび輻輳の効率的制御

【０００７】接続性

高速網では、ノードは総合的接続性を実現しなければならない。これには、ベンダーやプロトコルに関係なくユーザの装置を接続し、エンド・ユーザに他のどのような装置とも通信させることができる能力が含まれる。ネットワークは、データ、音声、ビデオ、ファックス、グラフィック、イメージを含む、どのようなタイプのトラフィックにも対応しなければならない。ノードは通信事業者の機能をすべて利用することができなければならず、複数のプロトコルに適合可能でなければならない。必要な変換はすべて、自動的かつエンド・ユーザにとって透過でなければならない。

【０００８】スループットおよび処理時間

高速パケット交換網の重要な要件の１つは、リアルタイム配信制約を満たすためと、音声とビデオの伝送のために必要なノード・スループットを実現するために、端末間遅延を短縮することである。リンク速度の向上に対して、それに釣り合った通信ノードの処理速度の向上はまだ実現されておらず、高速網に関する基本的な課題は各ノード内でのパケット処理時間を最小限にすることである。処理時間を最小限にし、高速／低誤り率技法を十分に利用するために、新しい広帯域ネットワーク・アーキテクチャが備える伝送機能と制御機能の大部分は、端末間ベースで行われる。フロー制御と、特に経路選択と帯域幅管理プロセスは、ネットワークのアクセス・ポイントによって管理され、それによって中間ノードはそれをあまり意識しなくても済むようになり、しかも中間ノードの役割が少なくなる。

【０００９】輻輳およびフロー制御

通信ネットワークは、効率的なパケット伝送が確実に行われるようにするために資源をネットワークの自由裁量で制限している。高速ネットワークを十分に活用するには効率的な帯域幅管理が必須である。１バイト当たりの伝送コストは年々低下し続けているが、帯域幅の需要が増大するに従い、伝送コストは将来の通信網を稼働させる主要な経費であり続ける可能性が高い。したがって、ネットワーク帯域幅を管理するためのフローおよび輻輳制御プロセス、帯域幅予約機構、ルーティング・アルゴリズムの設計にかなりの努力が費やされてきた。

【００１０】理想的なネットワークは、ネットワークに提供されるトラフィックに正比例した有用なトラフィックを伝送することができなければならず、これを最大伝送容量に達するまで行う。この限界を超えると、ネットワークは需要がどうであってもその最大容量で動作しなければならない。現実には、いくつかの理由により動作は理想とは異なっており、それらの理由はすべて過負荷状態の環境における資源の非効率的な割振りに関係する。

【００１１】動作を満足のゆくものにするためには、輻輳を回避するようにネットワークを実現しなければならない。最も単純な解決策は、装置の容量を大きめにして輻輳から離れた動作帯に位置するようにすることであることは明らかである。この解決策は、コストという明白な理由から一般には採用されず、ある程度の数の予防手段を適用する必要があり、その主なものは次の通りである。

・呼出し側加入者の送信データ伝送速度を受信側が吸収することができる速度に対応する速度に調整するフロー制御

・資源の過負荷を回避するためにネットワークに存在するパケットの数をグローバルに制限する負荷調整

・特定の資源における局所的輻輳を回避するために、ネットワークのすべてのリンクを介してトラフィックを公平に分散させる負荷バランシング

【００１２】輻輳制御

トラフィック特性

輻輳を回避し、パケット通信網における十分なトラフィック・フローを保証するために、ネットワークへのパケット送信元のアクセスを継続的に制御することが一般的である。トラフィック・アクセスの制御に成功するには、まず、トラフィックを正確に特徴づけて、そのトラフィックを伝送するのに十分な帯域幅を提供するようにすることが必要である。送信元の必要帯域幅の正確な推定を実現する単純な測定法は、「A Method for Capturing Traffic Behavior with SimpleMeasurements」（ダービー（Derby）他）という名称の米国特許第５２７４６２５号で教示されている。この出願では、トラフィックを特徴づけるために使用するパラメータは次の通りである。

・Ｒ－ビット／秒単位で表した着信トラフィックのピークビット伝送速度

・ｍ－ビット／秒単位で表した着信トラフィックの平均ビット伝送速度

・ｂ－秒単位で表したトラフィックの平均バースト期間

【００１３】しかし、実際のバースト期間を使用するの

ではなく、いわゆる「指数置換」技法を使用して、トラフィックが適切に動作する指数分布オン／オフ・プロセスであるとした場合と同じパケット紛失率になる同等のバースト期間を計算する。このような指数プロセスとは大きく異なるトラフィックの場合、この同等のバースト期間によって実際のトラフィックのはるかに正確な特徴づけが得られ、したがって、同じ伝送機構でより高いトラフィック密度が可能になる。

【００１４】漏れバケット

実際のトラフィック動作が当初の仮定から著しく逸脱している場合、この測定したパラメータを使用してネットワークへの信号源のアクセスを制御する。漏れバケット機構は、トラフィックが当初の仮定を超える場合にネットワークへのアクセスを制御し、しかもトラフィックが上記の当初の仮定の範囲内にある場合にはネットワークへのトラフィック・アクセスができるようにする１つの技法である。このような漏れバケット機構の１つは、「Rate-based Congestion Controlin Packet Communications Networks」（アフマディ（Ahmadi）他）という名称の米国特許第５３１１５１３号に記載されている。具体的には、この出願の漏れバケット機構は、一定期間に伝送することができる優先度の低いパケットの数を制限すると同時に、所与の時点で伝送される赤パケットの数に最小値を課すことによって、優先度の低いパケットによるネットワークの飽和を防止する。このような漏れバケット制御機構によって、パケット網の低優先度のスループットが最適化される。この漏れバケット機構では、優先度の高いトラフィックは当然、ほとんどあるいはまったく遅延なしに伝送される。

【００１５】トラフィック監視

上述の機構は、前記トラフィックが妥当に適切な動作をし、当初に仮定したトラフィック・パラメータにほぼ近い範囲内にある場合にのみ、トラフィックの制御に適している。しかしトラフィック管理システムは、適切に動作しない、当初に仮定したトラフィック・パラメータから大きく逸脱したトラフィックを扱うように構成されていなければならない。このような逸脱が長時間持続する場合、新しいトラフィック・パラメータに対応できるように、その接続に新しい接続帯域幅を割り当てなければならない。トラフィック動作の急激な変化に合わせたこのような制御システムの調整は、トラフィック測定値をフィルタリングしてトラフィック動作の過渡的変化をより長期の変化から区別する問題と、当初に仮定したトラフィック・パラメータを維持することができる範囲であってその範囲外では新しい接続帯域幅を要求しなければならない妥当な範囲を決定する問題を提起する。実際のトラフィックにとって広すぎる帯域幅は接続資源の無駄であり、帯域幅が小さすぎると過度のパケット紛失が発生することになる。副次的な問題としては、調整プロセスの容易さが妥当であることと、その実施を実現する際の計算要件が妥当であることがある。

【００１６】帯域幅測定および調整

「Dynamic Bandwidth Estimation and Adaptation for Packet CommunicationNetworks」（ダービー他）という名称の米国特許第５３５９５９３号では、その範囲内では調整が不要でその範囲外では新しい帯域幅割振りを要求しなければならない領域を定義することによる、トラフィック・パラメータの変化に合わせたトラフィック制御システムの動的調整が開示されている。具体的には、必要帯域幅は次のように調整される。

・測定値が、所望の最大パケット紛失率を超えることを示しているか、またはその接続上のトラフィックが伝送機構を共有する他の接続を不当に妨害し始める場合は、上方に調整する

・すべての接続のどのようなサービス品質保証も侵害することなく、ユーザとネットワークのバランスの両方にとって大幅な帯域幅の節約を実現することができる場合は下方に調整する

【００１７】調整領域に対するこれらの制限を、実効平均バースト期間ｂと平均ビット・レートｍの値に変換する。次に、測定実効平均バースト期間と平均ビット伝送速度をフィルタリングして、フィルタリングされた値が統計的に信頼性が高くなるように、すなわち、十分な数の生測定値が含まれるように保証し、予め選択した信頼レベルがその結果で保証されるようにする。トラフィックの平均ビット伝送速度を仮定すれば、この最低数の生測定値によって生測定値の収集に必要な時間の長さが決まる。この測定時間を使用して、漏れバケットへのデータ・ストリームの統計だけでなく、漏れバケットが着信トラフィックに与える影響も測定することができる。後者の測定によって、漏れバケットが提供されたトラフィックの分散をどれだけうまく扱うことができるか、従ってパケット紛失率を測定することができる。トラフィック・パラメータが所望の調整領域内に収まらない場合、トラフィック・パラメータの変化に対応するために、異なる帯域幅による新しい接続が要求される。

【００１８】「Dynamic Bandwidth Estimation and Adaptation for Packet CommunicationNetworks」（ダービー他）という名称の米国特許第５３５９５９３号で開示されている調整機構は、提供されたトラフィック変動が小さくて遅い場合に、絶えず妥当なトラフィック管理方法を保証する。しかし、トラフィック変動がより重要で高速になる場合、この機構にはいくつかの限界がある。その場合、この調整機構は収束により長い時間を要し、その結果、ネットワーク上の帯域幅の超過予約または予約不足になる。

【００１９】この調整機構の第２の限界は、実際では通常行われているように１つのプロセッサで複数の接続を監視する場合に現れる。接続によっては所与の期間内に他の接続よりも多くの帯域幅調整を必要とする場合があ

る。プロセッサの限られた処理能力の結果、公正さが失われ、他の接続を損なう可能性がある。

【００２０】

【発明が解決しようとする課題】したがって、本発明の目的は、大量かつ高速のトラフィックの変動のための帯域幅の動的な推定と調整を行う、米国特許第５３５９５９３号で開示されている機構を改良することである。

【００２１】他の目的は、複数の接続の調整を制御し、同じプロセッサによってサポートされるすべての接続間で公正さが確保されるようにすることである。

【００２２】

【課題を解決するための手段】本発明は、各ノードが１つまたは複数のリンクを処理する１つまたは複数のリンク・プロセッサを含む、送信元ノードから宛先ノードへのデジタル・トラフィックの伝送のために、伝送リンクによって相互接続された複数のノードを含むパケット交換通信網へのアクセスを動的に調整する方法およびシステムに関し、前記送信元ノードからのトラフィックの平均ビット伝送速度を測定するステップと、漏れバケット制御回路を使用して前記送信元ノードからネットワークへの前記トラフィックのフローを制御するステップと、前記漏れバケット制御回路によって前記ネットワークにもたらされるパケットの紛失率を測定するステップと、前記紛失率測定値をフィルタリングするステップと、前記同時平均ビット伝送速度および紛失率測定の値に対して調整領域を定義するステップと、前記調整領域内に収まらない前記平均ビット伝送速度および損失率測定の対に応答して、前記送信元ノードからの接続に割り振られた帯域幅の修正を要求するステップとを含み、帯域幅の修正を要求する前記ステップが、送信元ノード内の各リンク・プロセッサについて帯域幅修正要求の平均数を測定するステップと、送信元ノード内の同一プロセッサによって処理されるすべての接続のために、帯域幅修正要求の前記平均数に従って紛失率測定低域フィルタの帯域幅を調整するステップとを含む。

【００２３】

【発明の実施の形態】

高速通信

図２に示すように、通信システムの典型的なモデルは、専用回線、通信事業者提供サービス、または公衆データ・ネットワークを使用して高パフォーマンス・ネットワーク（２００）を介して通信するいくつかのユーザ・ネットワーク（２１２）から成る。各ユーザ・ネットワークは、企業サーバ（２１３）として使用される大型コンピュータ、ＬＡＮ（ローカル・エリア・ネットワーク２１４）に接続されたワークステーションまたはパーソナル・コンピュータを使用するユーザ・グループ、アプリケーション・サーバ（２１５）、ＰＢＸ（構内交換機２１６）、またはビデオ・サーバ（２１７）を相互接続する１組の通信プロセッサとリンク（２１１）であると言うことができる。これらのユーザ・ネットワークは、様々な施設に分散しており、広域伝送機構を介して相互に接続する必要があり、様々な手法を使用してデータ転送を編成することができる。アーキテクチャによっては各ネットワーク・ノードでデータ保全性を検査する必要があり、したがって伝送速度が低下するものがある。また他のアーキテクチャでは、本質的に高速データ転送を追求し、その目的のために、パケットの最終宛先に向かって流れるパケットを可能最高速度で処理するようにノード内の伝送、ルーティング、および交換技法が最適化される。

【００２４】本発明は本質的には後者の範疇に属し、具体的には以下の各段で説明する高速パケット交換網アーキテクチャに属する。

【００２５】高パフォーマンスパケット交換網

図２の概要図には、各ノードが幹線（２０９）と呼ばれる高速通信回線を使用して相互接続されている８つのノード（２０１～２０８）を含む高速パケット交換伝送システムが示されている。ユーザによる高速網へのアクセス（２１０）は、周縁部にあるアクセス・ノード（２０２～２０５）を介して実現される。これらのアクセス・ノードは１つまたは複数のポートを含み、各ポートは、ネットワークへの標準インタフェースのサポートと他の外部装置との間でネットワークを介してユーザ・データ・フローを伝送するために必要な変換とを行う外部装置を接続するアクセス・ポイントを提供する。たとえば、アクセス・ノード２０２は、３つのポートを介してそれぞれ構内交換機（ＰＢＸ）とアプリケーション・サーバとハブとにインタフェースし、隣接する中継ノード２０１、２０６、および２０８を使用してネットワークで通信する。

【００２６】交換ノード

各ネットワーク・ノード（２０１～２０８）は、着信データ・パケットが発信幹線で隣接中継ノードに向けて選択的にルーティングされるルーティング・ポイントを含む。このようなルーティングの決定は、データ・パケットのヘッダに含まれる情報に従って行われる。基本パケット・ルーティング機能に加えて、ネットワーク・ノードは次のような副次的サービスも提供する。

・ノードで発信されるパケットのルーティング経路の決定

・ネットワーク・ユーザおよび資源に関する情報の検索や更新などのディレクトリ・サービス

・リンク使用情報を含む、物理ネットワーク・トポロジの一貫性のあるビューを維持する

・ネットワークのアクセス・ポイントにおける資源の予約

【００２７】各ポートは、複数のユーザ処理装置に接続され、各ユーザ装置は他のユーザ・システムに送信するデジタル・データの送信元か、または他のユーザ・シス

テムから受信したデジタル・データを消費するためのデータ・シンクか、あるいは典型的にはその両方を含む。ユーザ・プロトコルの解釈と、ユーザ・データからパケット・ネットワーク（２００）での送信に適した形式のパケットへの変換と、これらのパケットをルーティングするヘッダの生成とが、ポートで稼働しているアクセス・エージェントによって実行される。このヘッダは、制御フィールドとルーティング・フィールドから成る。

・ルーティング・フィールドには、パケットをネットワーク（２００）を介してそのパケットの宛先である宛先ノードにルーティングするのに必要なすべての情報が入れられる。このフィールドは、指定ルーティング・モード（コネクション指向ルーティング・モードかコネクションレス・ルーティング・モードか）によっていくつかの形式をとることができる。

・制御フィールドには、他の情報の他に、ルーティング・フィールドの解釈に使用するプロトコルのコード化識別情報が入れられる。

【００２８】ルーティング・ポイント

図３に、図２に示すネットワーク・ノード（２０１～２０８）に見られるような典型的なルーティング・ポイント（３００）の概要ブロック図を示す。ルーティング・ポイントは、ルーティング・ポイントに着信するパケットが入る高速パケット交換機（３０２）を含む。このようなパケットは以下のように受信される。

・幹線アダプタ（３０４）を介して高速伝送リンク（３０３）で他のノードから。

・ポート（３０１）と呼ばれるアプリケーション・アダプタを介してユーザから。

【００２９】アダプタ（３０４、３０１）は、交換機（３０２）を使用してどのパケットをローカル・ユーザ・ネットワーク（３０７）に向けてまたは伝送リンク（３０３）に向けてノードからルーティングするかを、パケット・ヘッダ内の情報を使用して決定する。アダプタ（３０１および３０４）は、交換機（３０２）に送る前または後にパケットを待ち行列化するための待ち行列化回路を備える。

【００３０】ルート・コントローラ（３０５）は、ユーザが指定した所与の１組のサービス品質を満たし、通信経路を完成するために使用されるネットワーク資源の量が最小限になるように、ネットワーク（２００）を通る最適経路を算出する。次に、ルーティング・ポイントで生成されたパケットのヘッダを作成する。最適化基準には、中間ノードの数と、接続要求の特性と、経路内の幹線の使用と、当該接続のために指定されたサービス品質とが含まれる。

【００３１】ノードとノードに接続された伝送リンクに関する、ルーティングに必要な情報はすべてネットワーク・トポロジ・データベース（３０６）で保持される。安定状態では、あらゆるルーティング・ポイントがネットワークの同じビューを持つ。ネットワーク・トポロジ情報は、新しいリンクが活動化されたとき、ネットワークに新しいノードが追加されたとき、リンクまたはノードが除去されたとき、またはリンクの負荷が大幅に変化したときに更新される。このような情報は、資源が接続されているネットワーク・ノードから発信され、制御メッセージを使用して他のすべての経路サーバと交換されて、経路選択に必要な最新のトポロジ情報が提供される（このようなデータベース更新内容はネットワークのエンド・ユーザ間で交換されるデータ・パケットときわめて類似したパケットで伝達される）。ネットワーク・トポロジが絶え間ない更新によってすべてのノードで最新に維持されることにより、エンド・ユーザの論理接続（セッション）を中断することなく動的ネットワーク再構成が可能になる。

【００３２】パケット・ルーティング・ポイントへの着信伝送リンクは、ローカル・ユーザ・ネットワーク（２１０）内の外部装置からのリンクか、または隣接ネットワーク・ノード（２０９）からのリンク（幹線）を含むことができる。いずれの場合も、ルーティング・ポイントは同じように動作して各データ・パケットを受信し、それをパケット・ヘッダ内の情報で指定された別のルーティング・ポイントに転送する。高速パケット交換網は、１つのパケットの期間を除いてどの伝送機構またはノード機構もその通信経路専用とすることなく、任意の２つのエンド・ユーザ・アプリケーション間での通信を可能にするように動作する。このようにして、パケット・ネットワークの通信機構は、各通信経路の専用伝送リンクで可能なよりも格段に多くのトラフィックを伝送するように最適化される。

【００３３】ネットワーク制御機能

ネットワーク制御機能は、物理ネットワークの制御と割振りを行う機能である。各ルーティング・ポイントはルート・コントローラ（３０５）内に前述の１組の機能を持っており、それを使用してユーザ・アプリケーション間の接続の確立と保守を行う。ネットワーク制御機能には具体的には以下の機能が含まれる。

・ディレクトリ・サービス

・ネットワーク・ユーザおよび資源に関する情報の検索と維持を行う

・帯域幅管理

・帯域幅予約メッセージと保守メッセージの処理を行う

・リンクの現行予約レベルを監視する

・経路選択

・接続要件と現行使用レベルを考慮して、各新規接続のための最前の経路を選択する

・制御スパン・ツリー

・ネットワーク・ノード間のルーティング・ツリーの確立と維持を行う

・それを使用して、リンク使用状況を含む制御情報を

（並列して）配布する。
・新しいネットワーク構成またはリンク／ノード障害によって、ノードのトポロジ・データベースを更新する
・トポロジ更新
・スパン・ツリーを使用して、すべてのノードで論理ネットワークおよび物理ネットワークに関する情報（リンク使用状況情報を含む）の配布と維持を行う
・輻輳制御
・セットアップ時に確立されたネットワーク・ユーザとネットワークの間の帯域幅予約協定を守らせる
・実際の帯域幅を推定もり、接続の存続期間中に必要なら予約を調整する

【００３４】輻輳制御
ネットワーク制御機能は、ネットワークを介して確立されたすべての伝送接続に、サービス品質保証機能と、必要な場合は帯域幅保証を提供する。指定された帯域幅による伝送接続が設定されると、ネットワークと接続開始者との間の対話によって、その接続のために保証帯域幅が予約されるか、またはネットワーク資源がないために接続がブロックされる。セットアップが完了し、伝送が開始されると、輻輳制御機構が、バースト性を制御し、リンクのある程度の長期平均ビット伝送速度を保証することによって、ネットワークに送られるトラフィックが割り振られた帯域幅内に確実にとどまるようにする。接続が、接続セットアップ時に必要な帯域幅を指定する場合は、その接続はそれ自体の輻輳制御機構を必要とし、その接続にはそれ自体のネットワーク接続が割り当てられる。

【００３５】基本予防輻輳制御方法は、各接続のアクセス・ノードで稼働する漏れバケット機能から成る。この漏れバケット機能は、ユーザの予約レベルのトラフィックが限定された遅延と、中間ノードでの輻輳によるきわめて低い（10^{-6} のオーダーの）パケット紛失率とでネットワークを通過するようにユーザに保証することを目的とする。低／無パケット紛失を実現する最も単純な方法は、ユーザ接続の全帯域幅を予約することであろう。しかし、バースト性のユーザ・トラフィックの場合、この手法はネットワークでかなりの量の帯域幅を無駄に使う可能性がある。したがって、１つの手法はユーザが必要とする「同等容量」に等しい量の帯域幅を予約することである。

【００３６】基本概念は、予約機構が送信元特性とネットワーク状況を知って、予約のレベルを導き出すことである。この予約レベルは、ユーザが必要とする平均帯域幅と接続の最大容量との間に収まる。よりバースト性の高い接続の場合、よりバースト性の低い接続よりもこの予約レベルを高くして、同じ廃棄率を保証する必要がある。

【００３７】ほとんどのトラフィックは帯域幅予約された接続上を流れるため、自分で推定もることができないユーザのために必要帯域幅を推定もることが必要である。たとえば、顧客がＬＡＮサーバからネットワークに入るトラフィックの必要帯域幅を定義するのはかなり難しいであろう。したがって、ユーザ・トラフィックとリンクの使用量を推定もり、どのような測定値を使用するかを判断し、検出されたユーザの必要帯域幅の変化に合わせていつどのように漏れバケット・パラメータを変更するかを決めるためにどのようなフィルタを使用するかを判断するのに、かなりの作業が行われている。輻輳制御機構は、ユーザのトラフィック・ストリームを監視し、必要な場合は予約帯域幅に変更を加えて、ユーザ需要の増大に従って紛失率を保証したり、ユーザ需要の減少に従って帯域幅をより効率的に使用したりする。これに関する特定の課題は、帯域幅予約をあまり頻繁に調整するのを避けることである。これは、大幅な変更にはネットワークを介した新しい経路選択と帯域幅管理のフローが必要であり、頻繁な変更によってネットワーク・スラッシング条件が発生する可能性があるためである。

【００３８】接続要求
ネットワークでパケットを送信するために、送信元ノードから宛先ノードまでのネットワークを通る可能な経路またはルートを算出する必要がある。このルート上のどのリンクにも負荷がかかり過ぎないようにするために、新しい接続に十分な帯域幅が使用可能になるように保証するアルゴリズムに従ってルートを計算する。このような１つのアルゴリズムは、「Method and Apparatus for OptimumPath Selection in Packet Transmission Networks」（アフマディ他）という名称の米国特許第５２３３６０４号で開示されている。このようなルートが算出されると、ネットワークで接続要求メッセージが発信され、算出されたルートをたどり、新しい接続を反映するようにルートに沿った各リンクの帯域幅占有を更新する。

【００３９】図７に、前もって算出されたルートに沿って送信元ノードから宛先ノードに発信される接続要求メッセージのグラフを示す。接続メッセージは、前もって算出されたルートに沿って接続メッセージを送信するのに必要な情報が入ったルーティング・フィールド（７００）を含む。接続要求メッセージには、新しいパケット送信元の重要な統計特性を特徴づける接続要求ベクトル（７０１）も含まれ、それによってその新しい送信元を、ルートの各リンク上に直前に存在する信号と多重化することができる。後で詳述するように、この接続要求ベクトルには、パケット送信元を十分に特徴づけるのに必要なパラメータが比較的少ない。「Rate-based Congenstion in Packet Communications Networks」（アフマディ他）という名称の米国特許第５３１１５１３号に記載されているように、これらのパラメータには以下のものを含めることができる。
・Ｒ：送信元の最大ビット伝送速度

・ｍ：その速度の平均値
・ｂ：その送信元からのパケットの同等バースト期間
【００４０】接続要求ベクトル内の値を使用して、ルートの各リンクをテストしてそのリンクが新しい接続に実際に対応することができるかどうかを調べ、各リンクごとに別々に、新しい接続の追加を反映するようにそのリンクのリンク占有メトリックを更新する。ルートを算出してからリンク占有状況が変化している場合は、ルート上のいずれかのノードで接続が拒否されることがあり、送信元ノードに拒否が通知される。最後に、制御フィールド（７０２）には、接続の確立に使用される追加情報が含まれるが、本発明には直接関係がないので本明細書では詳述しない。接続を終了する場合は、図７と同じ形式を持つ接続除去メッセージが、除去する接続のルートに沿って送信される。次に、除去された接続のメトリックを差し引くことによって、各リンクのリンク占有がその接続の除去を反映するように更新される。
【００４１】送信元帯域幅管理
ネットワーク（２００）に送られるユーザ・トラフィックの各送信元について、図１に示す送信元帯域幅管理システムを設ける。これらの帯域幅管理システムをアクセス・ノードに配置し、通信するユーザ２者間の伝送の各方向にそのようなシステムを１つずつ設ける。このシステムはハード・ワイヤ接続した回路構成要素で実現することができるが、好ましい実施態様ではプログラムされたコンピュータを使用する。これはそのような実施態様の方が、改良に対応し、トラフィック・パターンの変化を反映するために、容易に修正することができるためである。
【００４２】図１に示す送信元帯域幅管理の詳細な説明に進む前に、以下の変数について定義する。
・Ｒ：ユーザ送信元が接続を開始するために要求する入力トラフィックの最大ビット伝送速度（ビット／秒単位）
・ｍ：ユーザ送信元が接続の開始または調整を行うために要求する入力トラフィックの平均ビット伝送速度（ビット／秒単位）
・ｂ：ユーザ送信元が接続の開始または調整を行うために要求する入力トラフィックの平均バースト期間（秒単位）
・ｔ：ｍフィルタとζフィルタ（１０５および１０９）の両方のサンプリング期間。フィルタは測定値を受け取り、ｔ秒ごとにフィルタリングされた出力値
【数１】

$$\hat{m}$$

は以降ｍハットと記載する。$_n$とξ$_n$を推定および調整モジュール（１０４）に報告する。
・m_n：期間ｔのｎ番目のサンプリング期間の入力トラフィックの平均ビット伝送速度の生測定値。
・ξ$_n$：期間ｔのｎ番目のサンプリング期間に漏れバケット・モジュール（１０７）で観察される赤マーク確率の生測定値。
・ｍハット$_n$：ｎ番目のサンプリング期間の終わりに入力トラフィックについて図１のビット伝送速度ｍフィルタ（１０５）でフィルタリングされた、平均ビット伝送速度ｍのフィルタリング済みの値。
・
【数２】

$$\hat{\xi}$$

は以降ξハットと記載する。
$_n$：ｎ番目のサンプリング期間の終わりに漏れバケットについて図１の赤マーク確率ξフィルタ（１０９）でフィルタリングされた、赤マーク確率のフィルタリング済み値。
・γ：図１の漏れバケットとモジュール（１０７）で現在使用している青トークン生成速度。青トークン伝送速度によって、青としてマークされたパケットをネットワークに発信することができる速度が決まる。ネットワークでこの接続のためにγ（同等容量）の帯域幅が予約されているものとみなす。
・Ｍ：図１の漏れバケット・モジュール（１０７）内の青トークン・プールの最大サイズ。青トークン・プールのサイズによって、ネットワークに発信される青パケットの長さが決まる。
【００４３】接続エージェント・モジュール
図２と関連させて図１で説明したように、ネットワーク（２００）を介して新しい接続をセットアップする場合、パケット送信元がトラフィック特性の初期推定を行う。この推定はリンク（１１３）で、リンク（１１２）で送られるサービス品質（ＱＯＳ）と共に図１の帯域幅管理システムに着信する。このサービス品質要件には以下のものが含まれる。
・許容可能損失率
・許容可能遅延
・リアルタイム配信要件
【００４４】これらの接続要件を接続エージェント（１０３）が経路選択コントローラ（１０２）に渡す。経路選択コントローラ（１０２）は、これらの要件をトポロジ・データベース（１０１）に記憶されている最新のネットワーク記述と共に使用して、これらの要件をすべて満たす帯域幅（同等容量）γとネットワーク（２００）を通る接続経路とを算出する。１つの最適な経路選択コントローラについては、「Method and Apparatus for Optimum Path Selection in Packet Transmission Networks」（アフマディ他）という名称の米国特許第５２３３６０４号に記載されている。算出されると、提案の接続経路が図７に示すメッセージのような接続要求メッセージにコード化され、帯域幅要求としてリンク（１１

０）でネットワーク（２００）に発信される。図７の帯域幅要求メッセージは、算出された接続経路を通り、経路に沿った各ノードで、接続の次のリンクで接続要求を満たすのに必要な帯域幅を予約するために使用される。

・算出された経路の接続の各リンクで十分な帯域幅が使用可能な場合、宛先ノードはその要求を受け取って新しい接続の受入れを返送する。

・トラフィック・パターンの変化により、経路のいずれかのリンクで使用可能な帯域幅が十分にない場合、接続要求の拒否が送信元エンド・ノードに返される

【００４５】これらの帯域幅応答は、否定か肯定かを問わず、リンク（１１１）で接続エージェント（１０３）に返送される。

・接続が拒否された場合、ユーザ送信元に通知され、後で再度接続が試行される。

・接続が受け入れられた場合、漏れバケット・モジュール（１０７）が活動化され、ユーザ・トラフィックのアクセスを制御する適切なパラメータが供給される。その後、ユーザはトラフィックの導入を開始する。

【００４６】漏れバケット・モジュール

送信元帯域幅管理システムは漏れバケット・モジュール（１０７）を含み、そこに入力リンクでユーザ・トラフィックが送られる。漏れバケット・モジュール（１０７）の出力は図２のネットワーク（２００）に送られる。漏れバケット・モジュール（１０７）では、パケットは、従来「赤」および「青」と呼ばれている少なくとも２つの異なる優先度クラスのうちの１つと共にネットワークに発信される。この場合、青の方がより優先度が高い。

・青パケットは、ネットワーク内で許容可能なレベルの遅延および紛失率に基づく所定のサービス・グレードが保証される。

・赤パケットには同じ保証がなく、輻輳が発生すると青＊パケットよりも先に廃棄される。

【００４７】漏れバケット機構でパケットに最適にマークを付ける方法は、「Rate-based Congestion Control in Packet Communications Networks」（アフマディ他）という名称の米国特許第５３１１５１３号で開示されている。漏れバケット・モジュール（１０７）の機能は、ネットワーク（２００）に入れる前にトラフィックを「整形」することである。当初に設けた統計記述に適合しないユーザ・パケットは、赤としてマークされるかまたは廃棄される。ピーク伝送速度Ｒと平均速度ｍと平均バースト期間ｂとで特徴づけられる接続の場合、４つのパラメータが計算され、漏れバケット・モジュール（１０７）で使用されて、接続の帯域幅需要がネットワークでその接続のために実際に予約されている帯域幅を超えないように制御する。

・γ：青トークン生成率

その値は以下の関係（１）によって求められる。

【数３】

$$\gamma = R\frac{y - X + \sqrt{(y-X)^2 + 4X\rho y}}{2y}$$

上式で、Ｘは接続の経路に沿った各幹線アダプタ（３０４）上の使用可能なバッファ空間の容量（ビット数単位）である。εはネットワーク内の目的最大パケット紛失率である。

ｙ＝Ｉｎ（１／ε）ｂ（１－ρ）Ｒ、及び

ρ＝ｍ／Ｒ　（ρは送信元の使用を示す）

【００４８】説明を簡単にするために、バッファ・サイズがすべて同じ（Ｘ）であり、各リンクの目的最大パケット紛失率が同じεであるものとする。

・Ｍ：最大青プール・サイズ

その値は以下の関係（２）によって求められる。

【数４】

$$M = Max\left[\frac{b(R-m)(R-\gamma)\gamma}{(\gamma-m)R}\ln\frac{R(\gamma-m)+\xi_T m(R-\gamma)}{\xi_T\gamma(R-m)}, Max\_packet\right]$$

上式で、ξ_Tは目的赤マーク率（好ましい実施態様ではξ_T＝０．０１）であり、Ｍａｘ＿ｐａｃｋｅｔはネットワーク・アクセスでのパケットの最大サイズを示す。

・赤トークン生成率

その他は青トークン生成率の分数に設定される。好ましい実施態様では、この分数は１０％に設定される。γは以下の関係（３）によって求められる。

γ_R＝０．１×γ

・M_R：最大赤プールサイズ

その値は以下の関係（４）によって求められる。

M_R＝Ｍ

【００４９】接続確立時、帯域幅量γが接続エージェント・モジュール（１０３）によってネットワークに予約され、漏れバケット・パラメータが初期設定される。

・青トークン・プールは、関係（２）によって求められるその最大値Ｍに設定され、関係（１）によって求められる速度γで絶えず最新化される。プールは毎秒γビットを受け取る。

・同様に、赤トークン・プールは関係（４）によって求められるその最大値M_Rに設定され、関係（３）で求められる速度γ_Rで絶えず最新化される。

【００５０】各新規着信パケットについて、漏れバケット・モジュール（１０７）はその青プール内に十分な青トークンがあるかどうかを調べる。ある場合、そのパケットには「青」のタグが付けられ、ただちにネットワークに送信される。ない場合、漏れバケット・モジュール（１０７）は、赤プールに十分なトークンがあるかどうかを調べる。ある場合、そのパケットには廃棄可能

（「赤」）のタグが付けられ、ネットワークに送信される。ない場合、そのパケットは廃棄されるか、または任意選択により、パケットを送信することができる十分な青または赤トークンをプールを入れることができる期間のあいだ、間隔があけられる。

【００５１】しかし、トラフィック特性が当初の交渉値内に留まっている場合、赤マーク機構は、保証された紛失率を保証するように十分に制限される。着信トラフィック特性が交渉値から大幅に逸脱している場合、推定および調整モジュール（１０４）が呼び出されて修正処置をとり、後述するように帯域幅予約を増大または減少させる。

【００５２】推定および調整モジュール

接続が受け入れられると、漏れバケット・モジュール（１０７）が活動化され、ユーザはトラフィックの導入を開始する。それと同時に、推定および調整モジュール（１０４）がその着信トラフィックを監視して、接続の存続期間中に着信トラフィック特性に大きな変化が起こっていないかどうか調べる。変化がある場合、推定および調整モジュール（１０４）は接続エージェント（１０３）に通知して、新しい帯域幅割振りを要求し、接続エージェント（１０３）に接続に必要な新しいトラフィック・パラメータを供給する。前と同様に、接続エージェント（１０３）は前記接続の帯域幅調整を要求するで新しい帯域幅要求をリンク（１１０）発信する。調整が受け入れられた場合、漏れバケット・パラメータがその新しいトラフィック特性で更新され、推定および調整モジュール（１０４）はその新しい特性を使用して着信トラフィックの監視を続ける。

【００５３】新しい接続ではなく新しい帯域幅割振りだけが要求されることに留意されたい。これによって、古い接続の終了と新しい接続のセットアップとに要するオーバーヘッドが省かれる。要求された追加帯域幅が使用可能でない場合、送信元ノードの送信者との当初の交渉に応じて、その接続は終了させられるかまたはより低い優先度が与えられる。

【００５４】帯域幅測定およびフィルタリング

図１を参照すると、測定モジュール（１０６）での着信トラフィックの平均ビット伝送速度m_nの測定は単純である。カウンタが、サンプリング期間中に受信したビット数をカウントし、その数を長さｔで割る。同様に、赤マーク率ξ_nはサンプリング期間ｔ中に赤マークされたパケットの数を、期間ｔ中に送信された合計パケット数で割った数に等しい。これらの生データをｔ秒ごとに、それぞれmフィルタとξフィルタ（１０５）および（１０９）に送る。mフィルタとξフィルタ（１０５および１０９）の機能は、平均ビット伝送速度m_nと赤マーク率ξ_nの過渡変化をフィルタリングして除去することである。フィルタ（１０５）および（１０９）は、それぞれ平均ビット伝送速度と赤マーク率をｔ秒ごとに報告する。各フィルタ（１０５）または（１０９）は、現行生測定値と直前のすべての測定値を、フィルタリング済み値の推定りに写像する。x_1、x_2、．．．．、x_nを生測定値とし、

【数５】

$$\hat{x}$$

は以下ｘハットと記載する。$_1$、ｘハット$_2$、．．．．、ｘハット$_n$を推定値とする（ここでｘはｍまたはξである）。フィルタ（１０５）および（１０９）の写像は任意の関数とすることができるが、本発明の好ましい実施態様ではこの写像は指数関数である。ｎ番目の推定値ｘハット$_n$は以下のように求められる。

ｘハット$_n$＝αｘハット$_{(n-1)}$　＋（１－α）x_n

上式で、フィルタ・パラメータαは、ゼロと１の間にあり（０＜α＜１）、上記の等式の２つの項の相対的信頼性を決定する。αの値は、ｍフィルタ（１０５）の場合は０．８に等しい定数に設定される。ξフィルタ（１０９）の場合、αの値は以下のように、生の値ξ_nがフィルタされた値ξハット$_n$よりも大きいかどうかによって決まる。ξハット$_n$＜ξ_nの場合は、α＝０．８（公称値）であり、それ以外の場合は、$\alpha=\alpha_s$である。この場合、α_sは後述するように監視モジュール（１１４）によってリンク（１１６）で供給される。

【００５５】平均ビット伝送速度および赤マーク率のフィルタリングされた値ｍハット$_n$およびξハット$_n$は、ｔ秒ごとに１回、推定および調整モジュール（１０４）に送られる。これらのフィルタリングされた値は推定よび調整モジュール（１０４）で適切な値と比較され、調整が必要かどうか、すなわち新しい要求が許可されるかどうかが判断される。この比較については、図４にグラフで開示されている調整領域を参照しながら説明する。

【００５６】調整領域

図４に、前述のようにしてネットワーク・ポートでモジュール（１０６）、（１０５）、（１０８）、および（１０９）を使用して推定もられた平均ビット伝送速度ｍまたは赤マーク率ξあるいはその両方の変化に応答して、接続の帯域幅を調節するために使用する領域を示す。図４には、二次元面の以下の３つの領域が含まれている。

・以下のように定義される上方調整領域（６０２）

ξハット$_n$＜ξ_H

上記でξ_Hは好ましい実施態様では５．１０$^{-2}$に等しい定数である。領域（６０２）は２つの部分領域に細分される。

・ｍハット$_n$≦γ（６０２ａ）

・ｍハット$_n$＞γ（６０２ｂ）

・以下のように定義される下方調整領域（６０１）

・ξハット$_n$＜ξ_L

・ｍハット$_n$＜γ

上記で、ξ_Lは好ましい実施態様では１０$^{-2}$に等しい定

数である。領域（６０１）は以下の２つの部分領域に細分される。

mハット$_n$≦β．ｍ（６０１ａ）

mハット$_n$＞β．ｍ（６０１ｂ）

上記でβは好ましい実施態様では定数０．３である。

【００５７】動的帯域幅調整

ｔ秒ごとに、推定および調整モジュール（１０４）はフィルタリングされた値mハット$_n$およびξハット$_n$の位置を調べ、調整領域に従って接続帯域幅を上方または下方に調整するか、あるいは調整しないことを決定する。この決定は、図５に示すアルゴリズムに従って行われる。

・（５０１）テストによって座標（mハット$_n$、ξハット$_n$）の点が面上のどこにあるかを調べる。

・（５１２）その点が「無調整」領域（６０４）にある場合、調整を試行せずにアルゴリズムを終了する。

・（５０５）その点が「上方調整」領域（６０２）にある場合、第２のテスト（５０５）によって点（mハット$_n$，ξハット$_n$）を部分領域の１つに配置する。

・（５０７）その点が部分領域（６０２ａ）にある場合、バースト・パラメータｂの新しい値が「Dynamic Bandwidth Estimation and Adaptation for Packet Communications Networks」（ダービー等）という名称の米国特許第５３５９５９３号で開示されている指数代入方式を使用して推定もられる。ｂは以下の関係（５）によって求められる。

【数６】

$$b=\frac{\dfrac{M(\gamma-\hat{m}_n)R}{(R-\hat{m}_n)(R-\gamma)\gamma}}{\ln\left[\dfrac{R(\gamma-\hat{m}_n)+\hat{\xi}_n\hat{m}_n(R-\gamma)}{\hat{\xi}_n\gamma(R-\hat{m})}\right]}$$

・（５０６）その点が部分領域（６０２ｂ）にある場合、バースト・パラメータｂの新しい値を以下のように算出する。

ｂ＝ｂ＿ｍａｘ

上式で、ｂ＿ｍａｘはこの実施態様が対応できる最大バースト・サイズである。好ましい実施態様では、ｂ＿ｍａｘ＝１０ｍｓである。

・（５０２）その点が「下方調整」領域（６０１）にある場合、カウンタｎ＿Ｌｏｗが増分され、テストされる（５０３）。

・（５１２）カウンタの更新された値が、好ましい実施態様では５をとる定数Ｎ＿Ｌｏｗより少ない場合、このアルゴリズムは完了する。カウンタ（５０２）の増加とテスト（５０３）の値によって、過度状態中に速すぎる下方調整が行われないようにする。

・（５０４）その点がＮ＿ＬＯＷ期間ｔの間、「下方調整」領域（６０１）にある場合、テスト（５０４）によって２つの部分領域（６０１ａ）または（６０１ｂ）のうちの一方内の点の位置を判断する。

・（５０８）その点が部分領域（６０１ａ）内にある場合、バースト・パラメータｂの新しい値を以下のように計算する。

ｂ＝ｂ／ｃ

上式で、ｃは定数＞１である（好ましい実施態様ではｃ＝２）。

・（５０７）その点が部分領域（６０１ｂ）内にある場合、バースト・パラメータｂの新しい値を式（５）を使用して計算する。

・（５０９）ステップ（５０６）、（５０７）、または（５０８）でバースト・パラメータｂの新しい値が求められたら、青トークン生成率γを以下のように計算する。

ｍ＝mハット$_n$

【数７】

$$\gamma=R\frac{y-X+\sqrt{(y-X)^2+4X\rho y}}{2y}$$

【００５８】・（５１０）次に、図４の領域が次のように更新される。

・「下方調整」領域（６０１）の上位境界（６０３）と「上方調整」領域（６０２）の中間境界（６０５）がγの新しい値に設定される。

・「下方調整」領域（６０１）の中間境界（６０４）がβ．ｍに設定される。

【００５９】・（５１１）図７の帯域幅要求メッセージはリンク（１１０）でネットワークに送信され、経路上のすべてのノードに配信されて、その接続のために予約された帯域幅が調整される。

【００６０】複数接続の調整制御および公正さ

上述のアルゴリズムは、「Dynamic Bandwidth Estiomation and Adaptation for Packet Communication Networks」（ダービー他）という名称の米国特許第５３５９５９３号で開示されている方法およびシステムの、大量かつ高速トラフィック変動の改良である。具体的には、本発明は次の２つの重要な機能をサポートする。

・プロセッサに処理機能があれば、プロセッサによって調整することができる接続の数のグローバル制御

・接続間の公正さ

【００６１】上記の機能は、図１に示す動的トラフィック管理機構の上部に実施される監視モジュール（１１４）によってサポートされる。

【００６２】調整制御

接続数のグローバル制御は以下のようにして実施される。各サンプリング期間ｔで、監視モジュール（１１４）はリンク（１１５．１）、（１１５．２）、．．．、（１１５．Ｎ）でｎ個の帯域幅要求を受け取る。この場合、

０≦ｎ≦Ｎ

21

であり、上記でNはプロセッサが処理する接続の合計数である。

【００６３】最後の期間の帯域幅要求の平均数

【数８】

$$\tilde{n}$$

は以降ｎティルドと記載する。は、フィルタリング操作によって以下のように推定もられる。

ｎティルド＝０．９９ｎティルド＋０．０１ｎ

【００６４】次に、フィルタリングされた値ｎティルドを所定の閾値と照合する。プロセッサの処理能力（毎秒の調整数）をN_oとして、以下のテストを行う。

・ｎティルド＜０．２５N_oの場合、α_s＝０．４である。フィルタ係数α_sを緩めて、ξフィルタ（１０９）によって推定もった平均赤マーク率の高速な変動を可能にするきわめて緩い値にする。

・０．２５N_o≦ｎティルド＜０．５N_oの場合、α_s＝０．６。α_sは赤マーク率ξハット$_n$の変動を遅くする緩い値に設定される。

・０．５N_o≦ｎティルド＜０．７５N_oの場合、α_s＝０．８。α_sはその公称値に設定される。

・０．７５N_o≦ｎティルドの場合、α_s＝０．９５。α_sは、図４の面における転位がきわめて遅くなるように、平均赤マーク率ξハット$_n$を実質的に凍結する厳格な値に設定される。

【００６５】次に、線（１１６）を介して係数α_sを赤マーク率ξフィルタ（１０９）に転送して特性を調整する。この操作によって接続間の公正さが向上する。実際に、単位時間当たりの帯域幅調整数に関して１つの接続が他の接続よりも要求が大きい場合、監視モジュール（１１４）によって算出される係数α_sが増大し、したがって図４の下方調整領域（６０１）内の接続の経路にはより多くの時間を要するようになり、さらにそれによって毎秒の平均帯域幅調整数が強制的にN_oに集中する。

【００６６】図６に、監視モジュールの原理をグラフで示し、帯域幅要求の平均数ｎティルドの時間変動を示す。上述のアルゴリズムに従ってフィルタ・パラメータα_sを制御する４つの領域が以下のように定義される。

・領域（８０１）：きわめて厳格なフィルタ係数α_s

・領域（８０２）：厳格なフィルタ係数α_s

・領域（８０３）：公称フィルタ係数α_s

・領域（８０４）：緩いフィルタ係数α_s

【００６７】調整の公正さ

接続間の公正さは以下のようにして実現される。アダプタがサポートする各接続ｉについて（０≦ｉ≦Ｎ）、プロセッサは、接続の現行動作を反映する公正変数F_iを維持する。この公正変数は、接続セットアップ時に以下のように初期設定される。

【数９】

22

$$F_i = \frac{1}{N_o}$$

【００６８】各サンプリング期間ｔに、プロセッサはすべての接続（ｉ＝１、．．．、Ｎ）について以下の操作を行う。

・まず、公正変数F_iを以下いずれかで更新する。

・接続ｉが新しい帯域幅要求を必要としない場合は、F_i＝０．９９F_i

・接続ｉが新しい帯域幅要求を必要とする場合は、F_i＝０．９９F_i＋０．０１

【００６９】次に、公正変数F_iをテストする。$F_i > \delta / N_o$の場合（ただし、δは好ましい実施態様では１である定数）、接続ｉは公正な接続とはみなされなくなり、したがってその帯域幅要求がどうであっても、カウンタF_iが限界δ / N_oより下に減少するまで調整されない。

【００７０】この機構は、１つの接続が平均して、接続当たりのプロセッサ公正割り当てと呼ぶことができる１／N_oより大きいプロセッサの計算容量の部分を使用するのを防ぐという点で、各接続間の公正さが確保されるようにする。１より大きいδの値を使用すると、プロセッサ資源の容量を超えた予約が行われる。

【００７１】まとめとして、本発明の構成に関して以下の事項を開示する。

【００７２】（１）各ノードが１つまたは複数のリンクを処理する１つまたは複数のリンク・プロセッサを含む、送信元ノードから宛先ノードへのデジタル・トラフィックの伝送のために伝送リンク（２０９）によって相互接続された複数（２０１．．２０８）のノードを含むパケット交換通信網（２００）へのアクセスを動的に調整する方法であって、前記送信元ノードからのトラフィックの平均ビット伝送速度を測定するステップ（１０６）と、漏れバケット制御回路を使用して前記送信元ノードからネットワークへの前記トラフィックのフローを制御するステップ（１０７）と、前記漏れバケット制御回路によって前記ネットワークにもたらされるパケットの紛失率を測定するステップ（１０８）と、前記紛失率測定値をフィルタリングするステップ（１０９）と、前記同時平均ビット伝送速度および紛失率測定の値に対して調整領域を定義するステップと、前記調整領域内に収まらない前記平均ビット伝送速度および損失率測定の対に応答して、前記送信元ノードからの接続に割り振られた帯域幅の修正を要求するステップとを含み、帯域幅の修正を要求する前記ステップが、送信元ノード内の各リンク・プロセッサについて帯域幅修正要求の平均数を測定するステップと、送信元ノード内の同一プロセッサによって処理されるすべての接続のために、帯域幅修正要求の前記平均数に従って紛失率測定低域フィルタの帯域幅を調整するステップとを含む方法。

（２）帯域幅修正要求の平均数を測定する前記ステップが、帯域幅修正要求測定値の前記平均数をフィルタリングするステップをさらに含むことを特徴とする、上記（１）に記載の方法。

（３）同じプロセッサへの帯域幅修正要求平均数が多くなるほど、低域フィルタ（１０９）の帯域幅が減少することを特徴とする、上記（１）または（２）に記載の方法。

（４）接続がそれに割り振られた帯域幅の修正を必要とする頻度が高いほど、リンク・プロセッサが前記要求に与える優先度が低くなり、接続がそれに割り振られた帯域幅の修正を必要とする頻度が低いほど、リンク・プロセッサが前記要求に与える優先度が高くなることを特徴とする、上記（１）ないし（３）のいずれか一項に記載の方法。

（５）上記（１）ないし（４）のいずれか一項に記載の伝送リンク（２０９）で相互接続された複数のノード（２０１．．２０８）を含むパケット交換通信網（２００）へのアクセスを調整する方法を実行する手段を含む通信ノード（３００）。

（６）上記（５）に記載の複数のノード（２０１．．２０８）を相互接続する複数の伝送リンクを含むパケット交換通信網（２００）。

【図面の簡単な説明】

【図１】本発明による動的トラフィック管理機構の概要を示す図である。

【図２】本発明で請求するノードを含む高速パケット交換網の典型的なモデルを示す図である。

【図３】本発明による高速ノードを示す図である。

【図４】本発明による、平均ビット伝送速度／実効バースト期間面における、その領域外では既存の接続のために新しい接続パラメータが要求される調整領域を示すグラフである。

＊【図５】図４に示す調整領域を使用して帯域幅を動的に調整するプロセスのフロー・チャートである。

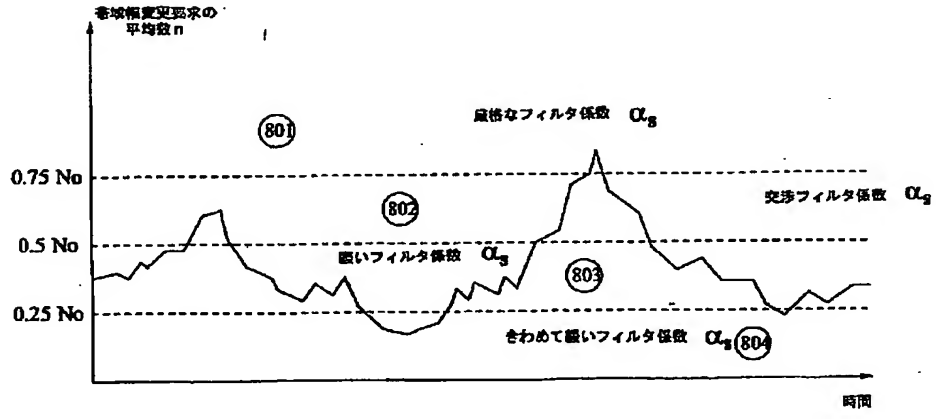
【図６】本発明の監視モジュールによるフロー制御実施例を示すグラフである。

【図７】本発明の動的トラフィック管理機構を使用して、初期接続と動的に変更された接続をセットアップするために使用することができる接続要求メッセージを示す図である。

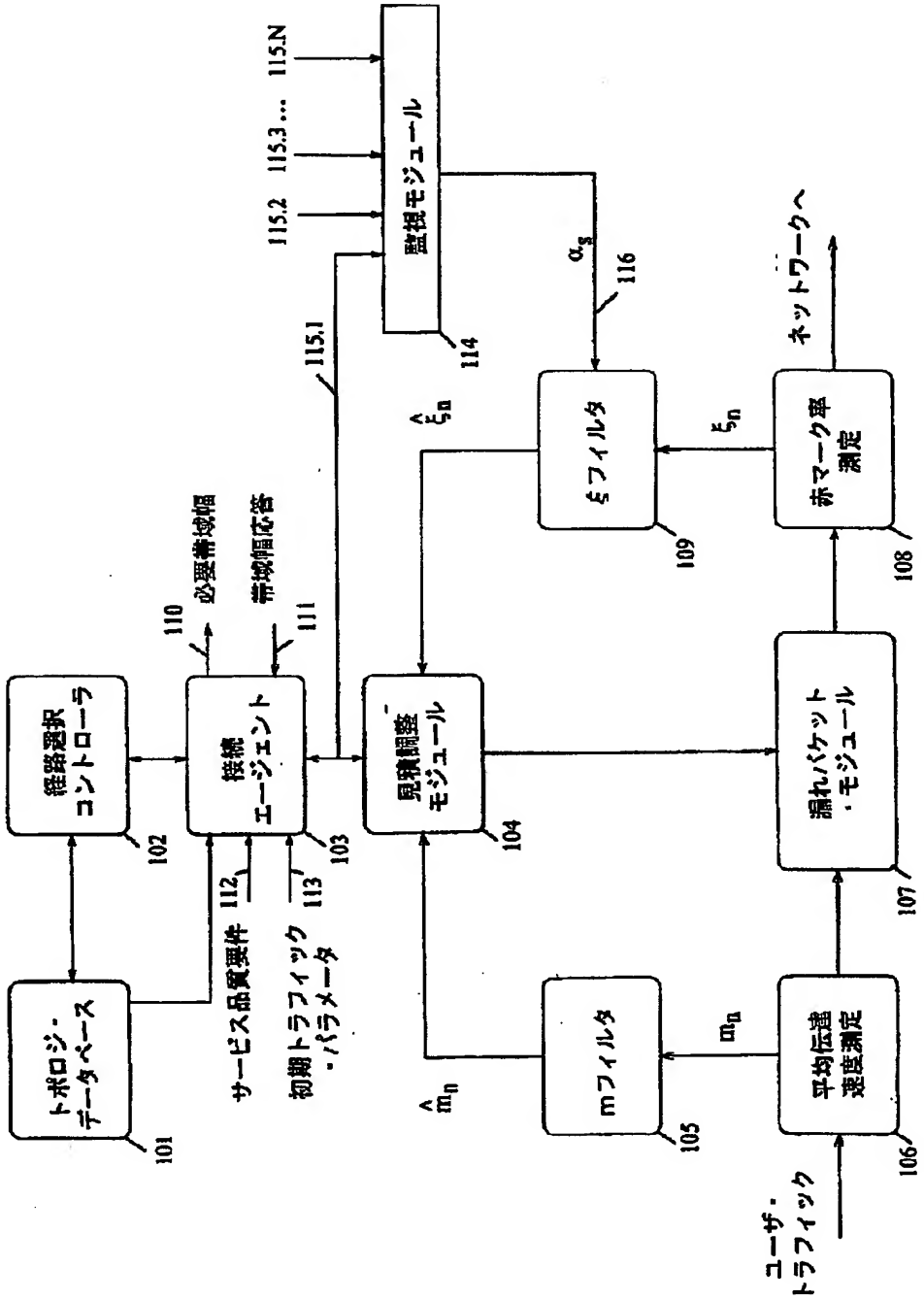
【符号の説明】

１０１	トポロジ・データベース
１０２	経路選択コントローラ
１０３	接続エージェント
１０４	推定および調整モジュール
１０５	mフィルタ
１０７	漏れバケット・モジュール
１０９	ξフィルタ
１１４	監視モジュール
２００	高パフォーマンス・ネットワーク
２０１	ノード
２０９	幹線
２１１	通信プロセッサおよびリンク
２１２	ユーザ・ネットワーク
２１３	企業サーバ
２１４	ローカル・エリア・ネットワーク
２１５	アプリケーション・サーバ
２１６	構内交換機
３００	ルーティング・ポイント
３０１	ポート
３０２	パケット交換機
３０３	高速伝送リンク
３０４	幹線アダプタ
３０５	ルート・コントローラ
３０６	ネットワーク・トポロジ・データベース

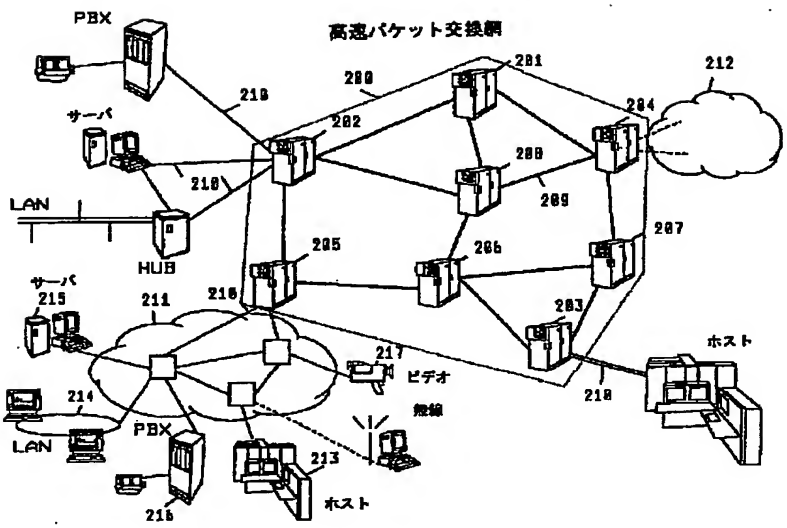
【図６】



【図１】


115.N
115.3 …
115.2
監視モジュール
114
115.1
α_s
116
ネットワークへ
$\hat{\xi}_n$
ξフィルタ
109
ξ_n
赤マーク率測定
108
必要帯域幅
110
帯域幅応答
111
経路選択コントローラ
102
接続エージェント
103
見積調整モジュール
104
漏れバケット・モジュール
107
トポロジ・データベース
101
サービス品質要件
112
初期トラフィック・パラメータ
113
$\hat{m}_n$
mフィルタ
105
m_n
平均伝達速度測定
106
ユーザ・トラフィック

【図２】

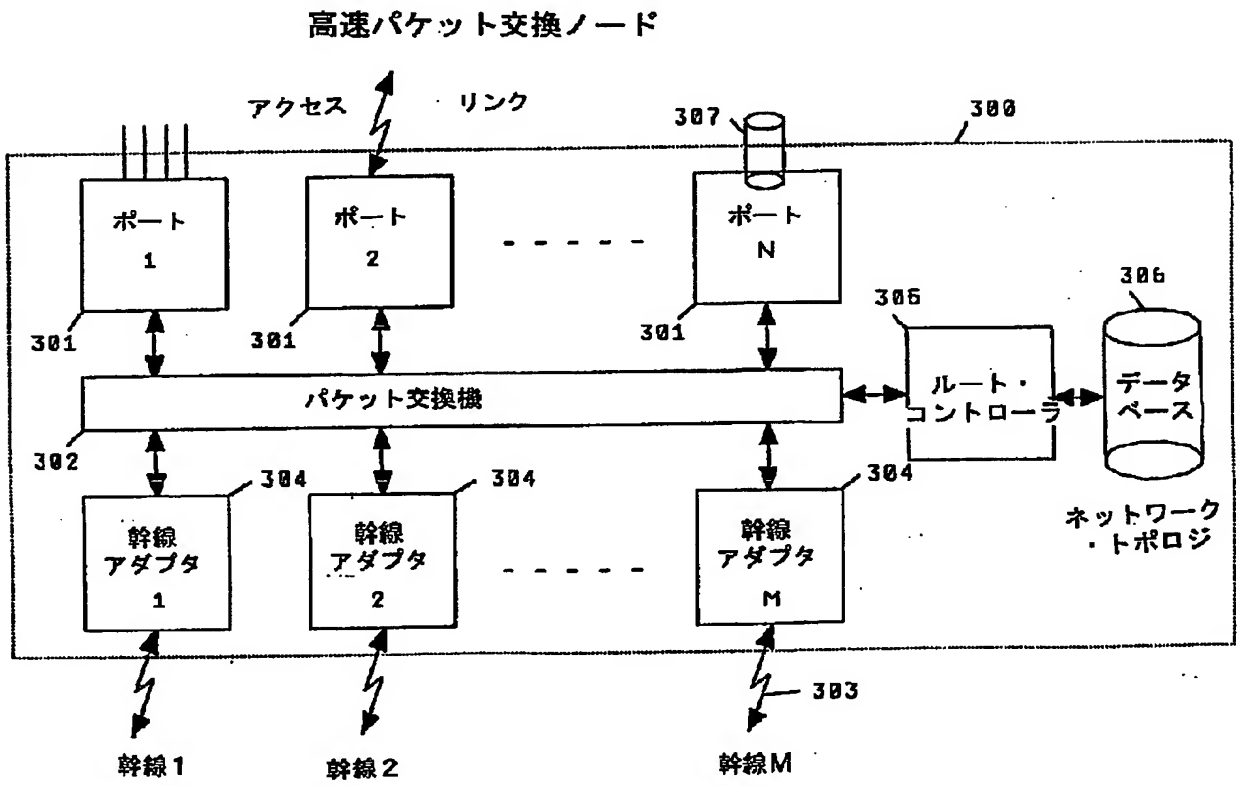


【図７】

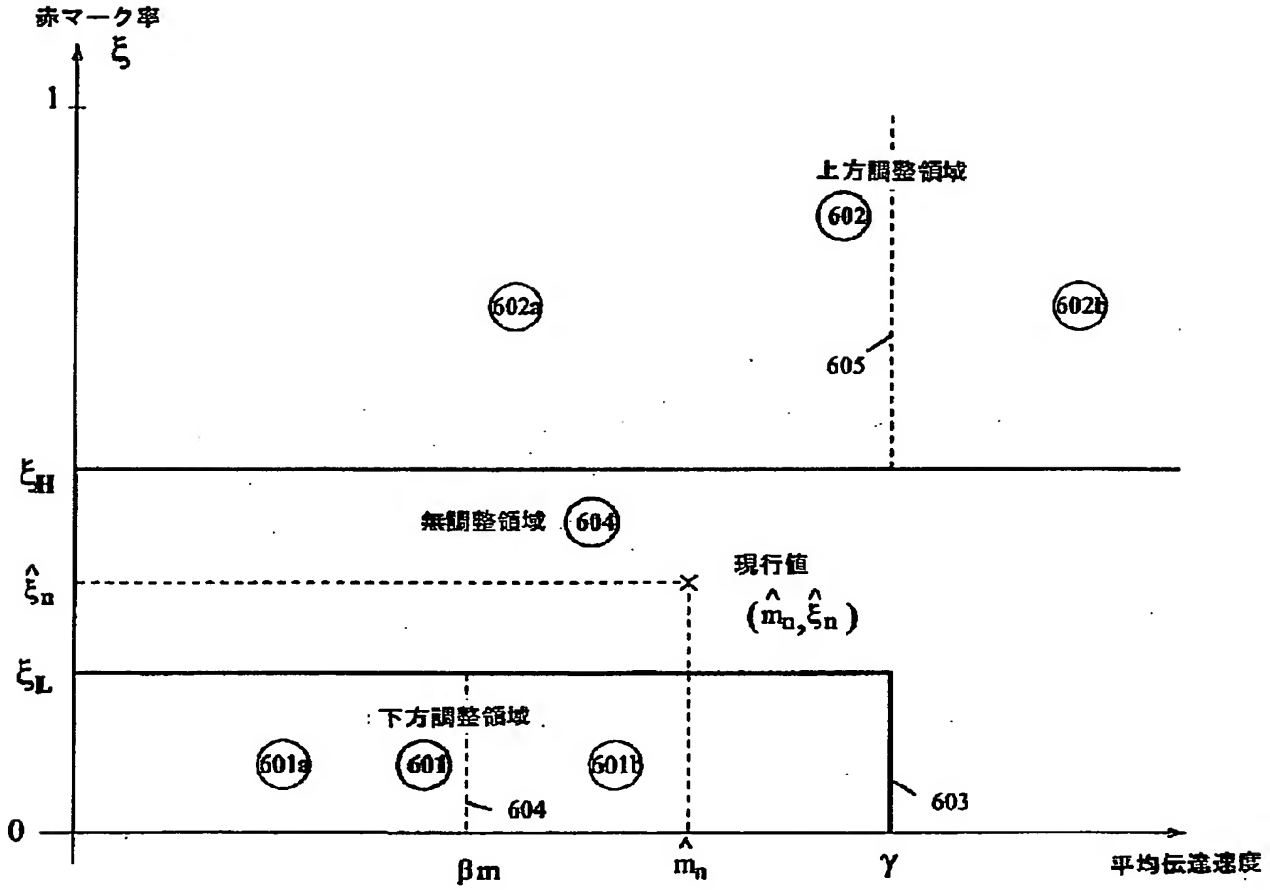
接続要求メッセージ（従来技術）

ルーティング・フィールド 700	接続要求ベクトル 701	制御フィールド 702

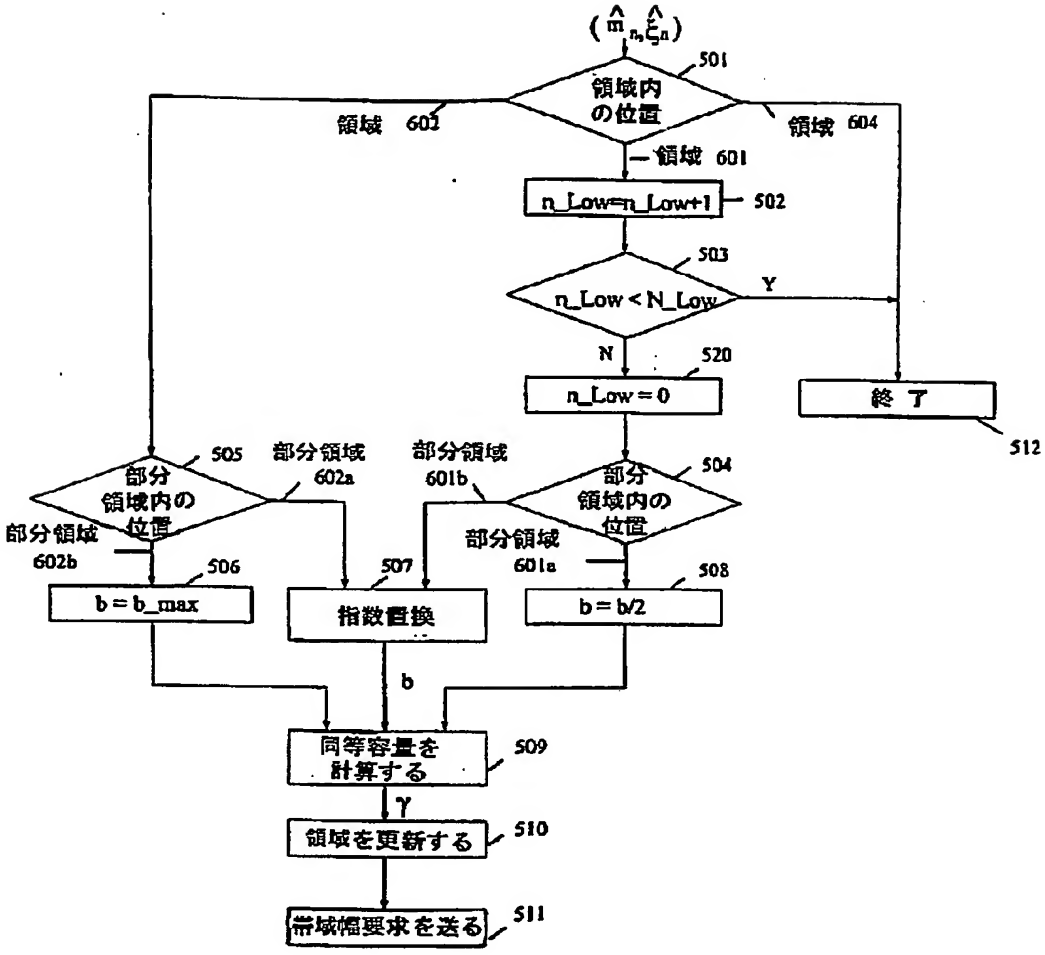
【図３】



【図４】


赤マーク率
ξ
1
上方調整領域
602
602a
602b
605
ξH
無調整領域
604
現行値
(m̂n, ξ̂n)
ξ̂n
ξL
下方調整領域
601a
601
601b
604
603
0
βm
m̂n
γ
平均伝達速度

【図５】



フロントページの続き

(72)発明者　ピエール＝アンドレ・フォリエル
フランス06700　サン・ローラン・デュ・ヴァルアヴニュ・エ・デシャム　60　レジダンス・マリアンヌ　ベー
(72)発明者　クロード・ギャラン
フランス06800　カニュ・シュル・メール　アヴニュ・デ・チュイリエール　56
(72)発明者　ステファン・ランジェル
フランス06600　アンティーブ　アヴニュ・バルキエ　6　「ル・ベル・ジュール」
(72)発明者　ローラン・ニコラ
フランス06270　ヴィユヌーヴ・ルーベレ・アモー・デュ・ソレイユ　レ・スピレ　ニュメロ20